



Configuring the Cisco ATA for H.323

This section describes how to configure the Cisco ATA to operate with the H.323 signaling image and how the Cisco ATA obtains the latest signaling image.

You can configure the Cisco ATA for use with H.323 with any of the following methods:

- By using a TFTP server—This is the Cisco-recommended method for deploying a large number of Cisco ATAs. This method allows you to set up a unique Cisco ATA configuration file or a configuration file that is common to all Cisco ATAs. The Cisco ATA can automatically download its latest configuration file from the TFTP server when the Cisco ATA powers up, is refreshed or reset, or when the specified TFTP query interval expires.
- By using manual configuration:
 - Voice configuration menu—This is the method you must use if the process of establishing IP connectivity for the Cisco ATA requires changing the default network configuration settings. These settings are CDP, VLAN, and DHCP. You also can use the voice configuration menu to review all IP connectivity settings. The voice configuration menu can also be used when Web access is not available.
 - Web-based configuration—This method is convenient if you plan to deploy a small number of Cisco ATAs in your network. To use this method, the Cisco ATA must first obtain IP connectivity, either through the use of a DHCP server or by using the voice configuration menu to statically configure IP addresses.

This section contains the following topics:

- [Default Boot Load Behavior, page 3-2](#)—This section describes the process that the Cisco ATA follows by default when it boots up. It is very important to understand this process because, if your network environment is not set up to follow this default behavior, you need to make the applicable configuration changes. For example, by default, the Cisco ATA attempts to contact a DHCP server for the necessary IP addresses to achieve network connectivity. However, if your network does not use a DHCP server, you must manually configure various IP settings as described in this section.
- [Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation, page 3-3](#)—This section includes a table of the parameters you can configure for VLAN and CDP settings.
- [Steps Needed to Configure the Cisco ATA, page 3-5](#)—This section provides tables that summarize the general configuration steps you must follow to configure the Cisco ATA.
- [Configuring the Cisco ATA Using a TFTP Server, page 3-7](#)—This section describes procedures for configuring the Cisco ATA by using a TFTP server, which is the recommended configuration method for the deployment of a large number of Cisco ATAs.
- [Voice Configuration Menu, page 3-15](#)—This section includes information on how to obtain basic network connectivity for the Cisco ATA and how to perform a factory reset if necessary.

- [Cisco ATA Web Configuration Page, page 3-18](#)—This section shows the Cisco ATA Web configuration page and contains a procedure for how to configure Cisco ATA parameters using this interface.
- [Web Interface Access-Control Configuration, page 3-20](#)
- [Refreshing or Resetting the Cisco ATA, page 3-20](#)—This section gives the procedure (via the Web configuration page) for refreshing or resetting the Cisco ATA so that your most recent configuration changes take effect immediately.
- [Upgrading the H.323 Signaling Image, page 3-21](#)—This section provides references to the various means of upgrading your Cisco ATA signaling image.

**Note**

The term *Cisco ATA* is used throughout this manual to refer to both the Cisco ATA 186 and the Cisco ATA 188, unless differences between the Cisco ATA 186 and Cisco ATA 188 are explicitly stated.

Default Boot Load Behavior

Before configuring the Cisco ATA, you need to know how the default Cisco ATA boot load process works. Once you understand this process, you will be able to configure the Cisco ATA by following the instructions provided in this section and in the sections that follow.

All Cisco ATAs are shipped with a boot load signaling-protocol image. However, because this image is not a fully functional signaling image, the image must be upgraded. The image is designed to be automatically upgraded by a properly configured TFTP server. To configure the Cisco ATA to automatically upgrade to the latest signaling image, see the [“Upgrading the Signaling Image from a TFTP Server”](#) section on page 8-1.

In addition, the Cisco ATA obtains its configuration file during the boot load process.

The following list summarizes the default Cisco ATA behavior during its boot-up process:

1. The Cisco ATA uses the Cisco Discovery Protocol (CDP) to discover which VLAN to enter. If the Cisco ATA receives a VLAN ID response from the network switch, the Cisco ATA enters that VLAN and adds 802.1Q VLAN tags to its IP packets. If the Cisco ATA does not receive a response with a VLAN ID from the network switch, then the Cisco ATA assumes it is not operating in a VLAN environment and does not perform VLAN tagging on its packets.

**Note**

If your network environment is not set up to handle this default behavior, make the necessary configuration changes by referring to the [“Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation”](#) section on page 3-3.

2. The Cisco ATA contacts the DHCP server to request its own IP address.

**Note**

If your network environment does not contain a DHCP server, you need to statically configure various IP addresses so that the Cisco ATA can obtain network connectivity. For a list of parameters that you must configure to obtain network connectivity, see [Table 3-5 on page 3-16](#). For instructions on how to use the voice configuration menu, which you must use to perform this configuration, see the [“Voice Configuration Menu”](#) section on page 3-15.

3. Also from the DHCP server, the Cisco ATA requests the IP address of the TFTP server.

- The Cisco ATA contacts the TFTP server and downloads the Cisco ATA release software that contains the correct signaling image for the Cisco ATA to function properly.



Note If you are not using a TFTP server, you need to manually upgrade the Cisco ATA to the correct signaling image. For information on this procedure, see the “[Upgrading the Signaling Image Manually](#)” section on page 8-2.

- The Cisco ATA looks for a Cisco ATA-specific configuration file (designated by the MAC address of the Cisco ATA and named `ata<macaddress>`) on the TFTP server and downloads this file if it exists.
- If the Cisco ATA does not find the `ata<macaddress>` configuration file, it looks for the `atadefault.cfg` configuration file and downloads this file if it exists. This file can contain default values for the Cisco ATA to use.



Note

When the Cisco ATA is downloading its DHCP configuration, the function button on the top panel blinks.

Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation

If you want the Cisco ATA to use a preconfigured VLAN ID instead of using the Cisco Discovery Protocol to locate a VLAN, or if you want to disable VLAN IP encapsulation, refer to [Table 3-1](#) for a reference to the parameters and bits you may need to configure. Use the voice configuration menu to configure these parameters. (See the “[Voice Configuration Menu](#)” section on page 3-15 for instructions on using this menu.) Also, refer to [Table 3-2](#) for a matrix on which VLAN-related parameters and bits to configure depending on your network environment.

Table 3-1 Parameters and Bits for Preconfiguring a VLAN ID

Parameter and Bits	Reference
OpFlags: <ul style="list-style-type: none"> Bit 4—Enable the use of user-specified voice VLAN ID. Bit 5—Disable VLAN encapsulation Bit 6—Disable CDP discovery. 	OpFlags, page 5-33
VLANSetting: <ul style="list-style-type: none"> Bits 0-2—Specify VLAN CoS bit value (802.1P priority) for TCP packets. Bits 3-5—Specify VLAN CoS bit value (802.1P priority) for UDP packets Bits 18-29—User-specified 802.1Q VLAN ID 	VLANSetting, page 5-34

Table 3-2 VLAN-Related Features and Corresponding Configuration Parameters

Feature	OpFlags Bit 4	OpFlags Bit 5	OpFlags Bit 6	VLANSetting Bits 18-29
Static VLAN	1	0	1	VLAN ID
CDP-acquired VLAN	0	0	0	N/A
No VLAN	N/A	1	N/A	N/A
No CDP	N/A	N/A	1	N/A
No CDP and no VLAN	0	1	1	N/A

N/A indicates that the variable is not applicable to the feature and the setting of this variable does not affect the feature.

Example

The following procedure shows you how to configure the OpFlags and VLANSetting parameters to allow the Cisco ATA to use a user-specified VLAN ID. In this example, the voice VLAN ID is 115 (in decimal format).

- Step 1** Set bits 4-6 of the OpFlags parameter to 1, 0, and 1, respectively. This setting translates to the following bitmap:

```
xxxx xxxx xxxx xxxx xxxx xxxx x101 xxxx
```

The remaining bits of the OpFlags parameter, using all default values, make up the following bitmap representation:

```
0000 0000 0000 0000 0000 0000 0xxx 0010
```

Therefore, the resulting value of the OpFlags parameter becomes the following bitmap representation:

```
0000 0000 0000 0000 0000 0000 0101 0010
```

In hexadecimal format, this value is 0x00000052.

- Step 2** Set bits 18-29 of the VLANSetting parameter to voice VLAN ID 115. This setting translates to the following bitmap

```
xx00 0001 1100 11xx xxxx xxxx xxxx xxxx
```

where 000001110011 is the binary representation of the decimal value 115.

The remaining bits of the VLANSetting parameter, using all default values, make up the following representation:

```
00xx xxxx xxxx xx00 0000 0000 0010 1011
```

Therefore, the resulting value of the VLANSetting parameter becomes the following bitmap representation:

```
0000 0001 1100 1100 0000 0000 0010 1011
```

In hexadecimal format, this value is 0x01cc002b.

**Note**

If you are using the voice configuration menu to set the parameters, you must convert hexadecimal values to decimal values. For example, the OpFlags setting of 0x00000052 is equivalent to 82 in decimal format, and the VLANSetting of 0x01cc002b is equivalent to 30146603 in decimal format.

Steps Needed to Configure the Cisco ATA

This section contains the following topics:

- [Basic Configuration Steps in a TFTP Server Environment, page 3-5](#)
- [Basic Configuration Steps in a Non-TFTP Server Environment, page 3-6](#)

Basic Configuration Steps in a TFTP Server Environment

[Table 3-3](#) shows the basic steps for configuring the Cisco ATA and making it operational in a typical H.323 environment, which includes a TFTP server.

Table 3-3 Basic Steps to Configure the Cisco ATA in a TFTP Environment

Action	Reference
1. Download the desired Cisco ATA release software zip file from the Cisco web site and store it on the TFTP server.	Setting Up the TFTP Server with Cisco ATA Software, page 3-7
2. Follow these basic steps to create a unique Cisco ATA configuration file, which actually entails creating two files: <ol style="list-style-type: none"> Create a Cisco ATA configuration text file that contains parameters that are common to all Cisco ATAs in your network. Create a unique Cisco ATA configuration text file that contains parameters that are specific to a Cisco ATA. Make sure to use an include command in the unique configuration file to pull in values from the common configuration file. Convert the unique configuration file to binary format. Place the unique binary configuration file on the TFTP server. 	Creating Unique and Common Cisco ATA Configuration Files, page 3-8
3. Optionally, create a default configuration file called atadefault.cfg, which the Cisco ATA will download from the TFTP server only if the unique Cisco ATA file called ata<macaddress> does not exist on the TFTP server.	atadefault.cfg Configuration File, page 3-12
4. Configure the upgradecode parameter so that the Cisco ATA will obtain the correct signaling image from the TFTP server when the Cisco ATA powers up.	Upgrading the Signaling Image from a TFTP Server, page 8-1
5. Configure the desired interval for the Cisco ATA to contact the TFTP server to check for a configuration-file update or an upgrade of the signaling image file.	Setting Up User IDs for the Cisco ATA, page 4-3


Table 3-3 Basic Steps to Configure the Cisco ATA in a TFTP Environment (continued)

Action	Reference
6. Configure the method with which the Cisco ATA will locate the TFTP server at boot up time.	Configuring the Cisco ATA to Obtain its Configuration File from the TFTP Server, page 3-12
7. Power up the Cisco ATA.	
8. If you make configuration changes to the Cisco ATA or upgrade the signaling image on the TFTP server, you can refresh the Cisco ATA so that these changes take effect immediately. Otherwise, these changes will take effect when the specified interval (CfgInterval parameter value) for the TFTP query expires.	Refreshing or Resetting the Cisco ATA, page 3-20

Basic Configuration Steps in a Non-TFTP Server Environment

[Table 3-4](#) shows the basic steps for configuring the Cisco ATA without using the TFTP server method.

Table 3-4 Basic Steps to Configure the Cisco ATA Without Using the TFTP Server Method

Action	Reference
<p>1. Download the desired Cisco ATA release software zip file from the Cisco web site:</p> <ol style="list-style-type: none"> If you are a registered CCO user, go to the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/ata186 Download the zip file that contains the software for the applicable release and signaling image you are using. The contents of each file are described next to the file name. Extract the files to the desired location on your PC. <p> Note The file that contains the protocol signaling image has an extension of .zup.</p>	
2. Manually upgrade the Cisco ATA to the correct signaling image.	Upgrading the Signaling Image Manually, page 8-2
3. Configure the Cisco ATA by using either one of the manual-configuration methods.	<ul style="list-style-type: none"> Voice Configuration Menu, page 3-15 Cisco ATA Web Configuration Page, page 3-18
4. Power up the Cisco ATA.	

Configuring the Cisco ATA Using a TFTP Server

The TFTP method of configuration is useful when you have many Cisco ATA because you can use a TFTP server for remote, batch configuration of Cisco ATAs. A TFTP server can host one unique configuration file for each Cisco ATA.


This section contains the following topics:

- [Setting Up the TFTP Server with Cisco ATA Software, page 3-7](#)
- [Configurable Features and Related Parameters, page 3-7](#)
- [Creating Unique and Common Cisco ATA Configuration Files, page 3-8](#)
- [atadefault.cfg Configuration File, page 3-12](#)
- [Configuring the Cisco ATA to Obtain its Configuration File from the TFTP Server, page 3-12](#)

Setting Up the TFTP Server with Cisco ATA Software

This section provides the procedure for the Cisco ATA administrator to obtain the correct Cisco ATA software and set up the TFTP server with this software.

Procedure

-
- Step 1** If you are a registered CCO user, go to the following URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/ata186>
- Step 2** Download the zip file that contains the software for the applicable release and signaling image you are using. The contents of each file are described next to the file name. Save the zip file onto a floppy disc.
-  **Note** The file that contains the protocol signaling image has an extension of .zup.
-
- Step 3** Extract the signaling files onto the TFTP server. This should be the same TFTP server that will contain the binary Cisco ATA configuration file that you create (either `ata<macaddress>` or `atadefault.cfg`).
-

Configurable Features and Related Parameters

[Table 4-1 on page 4-2](#) contains a list of all required H.323 parameters. These parameters must be properly configured for the Cisco ATA to work.

For descriptions of important Cisco ATA H.323 services that you can configure, and references to their configuration parameters, see the [“Important Basic H.323 Services” section on page 4-1](#) and the [“Additional H.323 Services” section on page 4-7](#).

[Table 4-4 on page 4-12](#) lists, in alphabetical order, various features that you can configure for the Cisco ATA. [Table 4-4 on page 4-12](#) also includes links to the related parameter that allows you to configure each of these features. Each link takes you to a detailed description of the parameter that includes its default values.

For an example of how to configure parameters for the TFTP Server configuration method, see the [“Creating Unique and Common Cisco ATA Configuration Files” section on page 3-8](#).

**Note**

Be sure to configure the UseSIP parameter to the value of 0 (its default) to enable the H.323 protocol.

Creating Unique and Common Cisco ATA Configuration Files

If you have many Cisco ATAs to configure, a good approach is to create two configuration files:

- One file that will contain only parameter values unique to a specific Cisco ATA.
- One file for parameters that will be configured with values common to a group of Cisco ATAs. If this file is updated, all Cisco ATA devices in this common group can obtain the new configuration data in a batch-mode environment.

The following procedure demonstrates the steps needed to create these configuration files.

**Note**

The parameters used in this section help illustrate the process of creating a unique Cisco ATA configuration file, and do not include all required H.323 parameters in the examples. See [Chapter 5, “Parameters and Defaults,”](#) for complete listings and descriptions of required parameters and additional configurable features. Also, refer back to [Table 3-3 on page 3-5](#) for all main configuration steps.

Procedure

Step 1 Use the example_uprofile.txt file as a template for creating a text file of values that are common to one group of Cisco ATAs. The example_uprofile.txt file is included in the software-release zip file and contains all default values. This file is shown without its annotations in the [“Configuration Text File Template” section on page 5-2](#).

Copy the example_uprofile.txt file and save it with a meaningful name, such as *common.txt*.

Step 2 Configure all common parameters by editing the text file as desired. For example, you might configure some parameters as follows:

```
ToConfig:0
UseTftp:1
DHCP:1
TftpURL:10.10.10.1
UseSIP:0
```

**Tip**

It is helpful to always include the parameter/value of ToConfig:0 in the Cisco ATA configuration file so that every time this file is downloaded to the Cisco ATA, it will set ToConfig to 0, which the appropriate value for this parameter once the Cisco ATA has been configured. If ToConfig is 1, the Cisco ATA will continue to unnecessarily contact the TFTP server.

The settings in this example indicate that a group of Cisco ATAs is using the TFTP server with an IP address of 10.10.10.1 to obtain their configuration files. These Cisco ATAs will use a DHCP server to obtain their own IP addresses but not to obtain the TFTP server IP address (because the TftpURL parameter has a configured value).

Step 3 Save your changes.

- Step 4** Use the `example_uprofile.txt` file again, this time as a template for creating a text file of values that are specific to one Cisco ATA. For example, you might configure the following parameters:

```
UserID:8530709
GkorProxy:192.168.1.1
```

Save this file of Cisco ATA-specific parameters as:

```
ata<macaddress>.txt
```

where *macaddress* is the non-dotted hexadecimal version of the MAC address of the Cisco ATA you are configuring. This non-dotted hexadecimal MAC address is labeled on the bottom of most Cisco ATAs next to the word “MAC.” The file name must be exactly 15 characters long. (However, if this filename is supplied by the DHCP server, the name can be as long as 31 characters and can be any name with printable ASCII characters.)

If necessary, you can obtain the non-dotted hexadecimal MAC address by using the `atapname.exe` command. For information on using the `atapname.exe` command, see the [“Using atapname.exe Tool to Obtain MAC Address” section on page 3-10](#). That section includes an example of a dotted decimal MAC address and its corresponding non-dotted hexadecimal address.



Note The `ata<macaddress>.txt` file should contain only those parameters whose values are different from the file of common parameters. Parameter values in the `ata<macaddress>` configuration file will overwrite any manually configured values (values configured through the web or voice configuration menu) when the Cisco ATA powers up or refreshes.

- Step 5** On the top line of the `ata<macaddress>.txt` file, add an **include** command to include the name of the common-parameters file, and save the file.

```
include:common.txt
UserID:8530709
GkorProxy:192.168.1.1
```

- Step 6** Run the `cfgfmt.exe` tool, which is bundled with the Cisco ATA software, on the `ata<macaddress>.txt` text file to generate the binary configuration file. If you wish to encrypt the binary file for security reasons, see the [“Using the EncryptKey Parameter and cfgfmt Tool” section on page 3-11](#).

The syntax of the `cfgfmt` program follows:

Syntax

```
cfgfmt [-eRC4Password] -tpTagFile input-text-file output-binary-file
```

- `-eRC4Password` is the optional RC 4key to encrypt the binary TFTP file provided by the `cfgfmt` program (up to eight alphanumeric characters).
- `pTagFile` is the command used to specify the *ptag.dat* file that is provided with the Cisco ATA software version you are running. Search on the keyword *ptag* to find the complete name of the *ptag* file that is included with the Cisco ATA software for the signaling protocol you are using. Be sure this file resides in the same directory from which you are running the `cfgfmt` program. The *ptag.dat* file is used by `cfgfmt.exe` to format a text input representation of the parameter/value pairs to its output binary representation. `input-text-file` is the input text file representation of the Cisco ATA configuration file.
- `input-text-file` is the input text file representation of the Cisco ATA configuration file.
- `output-binary-file` is the final output binary file that Cisco ATA uses as the TFTP configuration file.

Example

```
cfgfmt -tptag.dat ata0a141e28323c.txt ata0a141e28323c
```

This example is based on a Cisco ATA MAC address of 10.20.30.40.50.60, which converts to the two-digit, lower-case hexadecimal representation of each integer as 0a141e28323c.

When you convert the ata<macaddress>.txt file to a binary file, the binary file will merge the two text files to form one Cisco ATA-specific binary configuration file for your Cisco ATA.

If the same parameter is configured with different values in these two files, the value in the ata<macaddress>.txt file takes precedence over the value in the common.txt file.

Step 7 Store the binary configuration file in the TFTP server root directory.

When the Cisco ATA powers up, it will retrieve its unique configuration file from the TFTP server.

Step 8 If you want to make configuration changes after boot up, repeat the process of creating or editing the text files containing the desired parameters, then converting the ata<macaddress>.txt text file to the binary file and storing the binary file on the TFTP server. For the configuration changes to take effect immediately, refresh the Cisco ATA. (See the [“Refreshing or Resetting the Cisco ATA”](#) section on page 3-20.)

After being refreshed, the Cisco ATA will download the updated ata<macaddress> configuration file.



Note If you do not perform a refresh procedure, the Cisco ATA will update its configuration the next time it contacts the TFTP server, which is based on the configured value of the CfgInterval parameter.

Using atapname.exe Tool to Obtain MAC Address

This bundled tool is useful for converting the dotted decimal version of the Cisco ATA MAC address (available on the Cisco ATA Web configuration page or from the voice configuration menu code **24#**) to its default Cisco ATA profile name. This name has the following format:

```
ataxxxxxxxxxxxx
```

where each *xx* is the two-digit, lower-case hexadecimal representation of each integer in the dotted, decimal version of the Cisco ATA MAC address. This is the name you use for the unique Cisco ATA binary configuration file.

The following command and output show an example of this command.

Command Example

```
atapname.exe 10.20.30.40.50.60
```

Command Output

```
ata0a141e28323c
```



Note The same functionality is available from the voice configuration menu (voice menu code **84#**), which will announce the Cisco ATA profile name.

Using the EncryptKey Parameter and cfgfmt Tool

The EncryptKey parameter encrypts binary files being transferred over TFTP. You can change this key for each Cisco ATA, so that only one specific Cisco ATA can decode the information.

By default, the Cisco ATA-specific `ata<macaddress>` configuration file is not encrypted. If encryption is required, however, you must manually configure the EncryptKey parameter before you boot up the Cisco ATA so that the TFTP method is secure. Use either the voice configuration menu (see the [“Voice Configuration Menu” section on page 3-15](#)) or the Cisco ATA web configuration page (see the [“Cisco ATA Web Configuration Page” section on page 3-18](#)) to configure the EncryptKey parameter.



Note

Because the factory-fresh ATA cannot accept encrypted configuration files, the first unencrypted file, if intercepted, can easily be read. (You would still have to know the data structure format in order to decode the binary information from the unencrypted file.) Therefore, the new encryption key in the unencrypted file can be compromised.

Set the EncryptKey parameter to a nonzero value. When this value is nonzero, the Cisco ATA assumes that the binary configuration file on the TFTP server is to be encrypted with this key by means of the RC4 cipher algorithm. The Cisco ATA will use this key to decrypt the configuration file.

The Cisco ATA EncryptKey parameter and the encryption key used in the `cfgfmt` tool command syntax must match.



Note

For security reasons, Cisco recommends that you set the `UIPassword` parameter (if desired) in the configuration file and not by using one of the manual configuration methods.

The `cfgfmt.exe` syntax affects how the EncryptKey parameter is used, as shown in the following examples. In these examples, `input_text` is the `ata<macaddress>.txt` file that you will convert to binary to create the `ata<macaddress>` configuration file for the Cisco ATA; `output_binary` is that binary `ata<macaddress>` file, and `Secret` is the encryption key.

Syntax examples

- `cfgfmt -tpTagFile input-text-file output-binary-file`

If `input-text-file` sets the Cisco ATA EncryptKey parameter to 0, then `output-binary-file` is not encrypted. If the `input-text-file` sets EncryptKey to a non-zero value, then `output-binary-file` is encrypted with that value.

- `cfgfmt -eSecret -tpTagFile input-text-file output-binary-file`

If the Cisco ATA EncryptKey parameter has the value of 0 or is not included in `input-text-file`, the `Secret` is used to encrypt the `output-binary-file`. If `input-text-file` sets the Cisco ATA EncryptKey parameter to a nonzero value and the `-e` option is used, then `output-binary-file` is encrypted with the EncryptKey parameter set in `input-text-file` and `Secret` is ignored.

- `cfgfmt -E -tpTagFile input-text-file output-binary-file`

The `-E` (uppercase) option means that any value specified for the Cisco ATA EncryptKey parameter in `input-text-file` is ignored. However, because `Secret` is not specified in this example, `output-binary-file` is not encrypted. Nevertheless, the EncryptKey parameter and its value, if specified in `input-file-text`, will be included in `output-binary-file` for possible encryption at a later time.

- `cfgfmt -E -eSecret -tpTagFile input-text-file output-binary-file`

The -E (uppercase) option means that any value specified for the Cisco ATA `EncryptKey` parameter in `input-text-file` is ignored and the `output-binary-file` is encrypted with the `Secret` key. However, the `EncryptKey` parameter and its value, if specified in `input-text-file`, will be included in `output-binary-file`.

atadefault.cfg Configuration File

You can create a configuration file, called `atadefault.cfg`, that is common to all Cisco ATAs. This configuration file is applied to a Cisco ATA only if a unique configuration file (`ata<macaddress>`) does not exist for the Cisco ATA on the TFTP server during the Cisco ATA power-up procedure.

You can use the `atadefault.cfg` file to provide limited functionality for when you first install the Cisco ATA. For example, if your service provider provides the ethernet connection and VoIP telephony service, you may need to call customer service to activate the service. If the `atadefault.cfg` file is configured to provide a direct connection to the customer service center, you can simply pick up the telephone and wait to be connected without using your regular phone.

The following procedure illustrates how to create the Cisco ATA default configuration file, convert it to the required binary format that the Cisco ATA can read, and store it on the TFTP server so that the Cisco ATA will download it during the boot-up process:

Procedure

-
- Step 1** Make a copy of the `example_uprofile.txt` file and rename it `atadefault.txt`.
 - Step 2** Make the desired configuration changes by editing the `atadefault.txt` file, then save the file.
 - Step 3** Convert the `atadefault.txt` file to a binary file by running the `cfgfmt.exe` tool, which is bundled with the Cisco ATA software.



Note Be sure to name the output file `atadefault.cfg`.

- Step 4** Store the binary `atadefault.cfg` configuration file in the TFTP server root directory.
- During the boot-up process, the Cisco ATA will download this file as its configuration file unless it first finds a Cisco ATA-specific configuration file named for the MAC address of the Cisco ATA.
-

Configuring the Cisco ATA to Obtain its Configuration File from the TFTP Server

This section describes three methods for how the Cisco ATA contacts the TFTP server to obtain its configuration file:

- [Using a DHCP Server, page 3-13](#)
 - The Cisco ATA contacts the DHCP server, which provides the IP address of the TFTP server
 - The Cisco ATA uses the DHCP server but the DHCP server does not know about the TFTP server
- [Without Using a DHCP Server, page 3-14](#)

Using a DHCP Server

When using a DHCP server, configuration settings vary depending on whether or not the DHCP server is under the control of the Cisco ATA system administrator or the service provider. The simplest configuration is when the DHCP server is under the control of the Cisco ATA administrator, in which case the DHCP server provides the IP address of the TFTP server. Depending on who controls the DHCP server, follow the applicable configuration procedure:

- [Procedure if DHCP Server is Under Control of Cisco ATA Administrator, page 3-13](#)
- [Procedure if DHCP Server is not Under Control of Cisco ATA Administrator, page 3-13](#)

This section also includes the topic:

- [Other DHCP Options You Can Set, page 3-14](#)

**Note**

If no DHCP server is found and the Cisco ATA is programmed to find one, the function button continues to blink.

Procedure if DHCP Server is Under Control of Cisco ATA Administrator

Procedure

Step 1 On the DHCP server, set one of the following two options:

- DHCP option 150 (TFTP server IP address)
- Standard DHCP option 66 (TFTP server name)

If you use DHCP option 150, the Cisco ATA will ignore DHCP option 66. However, if you use DHCP option 66, you must turn off DHCP option 150 or set its value to 0.

**Note**

You can turn off the DHCP option 150 request by using the Cisco ATA OpFlags parameter (see the [“OpFlags” section on page 5-33](#)).

Step 2 Make sure to use default values for the following Cisco ATA parameters:

- TftpURL=0
- UseTftp=1
- DHCP=1

This completes the parameter settings and DHCP options you need to configure for this procedure. The Cisco ATA will contact the DHCP server for the IP address of the TFTP server that contains the Cisco ATA configuration file.

Procedure if DHCP Server is not Under Control of Cisco ATA Administrator

This is the procedure to use if the DHCP server is not under the control of the Cisco ATA administrator, which means that the URL of the TFTP server must be manually configured.

Procedure

- Step 1** Using the voice configuration menu, set the parameter TftpURL to the IP address or URL of the TFTP server. For more information on setting the TftpURL parameter, see the [“TftpURL” section on page 5-5](#). For information about using the Cisco ATA voice configuration menu, see the [“Voice Configuration Menu” section on page 3-15](#).



Note If you are not using a DHCP server to provide the TFTP server location, you *must* manually configure the TftpURL. You can do this by using the voice configuration menu without first obtaining network connectivity for the Cisco ATA. If you want to configure this value using the Web configuration page, you first must obtain network connectivity by using the voice configuration menu to statically configure IP address information (see the [“Voice Configuration Menu” section on page 3-15](#)).

- Step 2** Use the default value of 1 for the Cisco ATA parameter DHCP.

- Step 3** Use the default value of 1 for the Cisco ATA parameter UseTftp.

This completes the parameter settings you need to configure for this procedure. The Cisco ATA will contact the manually configured TFTP server that contains the Cisco ATA configuration file.

Other DHCP Options You Can Set

The following parameters can also be configured with DHCP:

- Boot file name of DHCP header—The ata<macaddress> binary Cisco ATA configuration file, which can have a maximum of 31 characters and can be any name with printable ASCII characters
- Client PC address
- DHCP option 1—Client Subnet Mask
- DHCP option 3—Routers on the client’s subnet
- DHCP option 6—One or two Domain Name servers
- DHCP option 42—One or two Network Time Protocol servers
- DHCP option 43—Set this option to identify the protocol (for example, **H.323**)
- DHCP Option 60 (DHCP_VENDOR_CLASS_ID)—Use this parameter to identify the type of Cisco ATA box (**ATA186** or **ATA188**).

Without Using a DHCP Server

Use the following procedure if you are not using a DHCP server in your environment but are still using a TFTP server to obtain the Cisco ATA configuration file:

Procedure

- Step 1** Set the DHCP parameter to 0.
- Step 2** Set the UseTFTP parameter to 1.
- Step 3** Set the Cisco ATA parameter TftpURL to the IP address or URL of the TFTP server. For more information on setting the TftpURL parameter, see the [“TftpURL” section on page 5-5](#).

**Note**

If you are not using a DHCP server to provide the TFTP server location, you must manually enter the TftpUrl using either the voice configuration menu or the Web configuration page.

Step 4 If you have done already done so, statically configure the following parameters using the voice configuration menu (see the [“Voice Configuration Menu”](#) section on page 3-15). These are the parameters you need to configure for the Cisco ATA to obtain network connectivity:

- StaticIP
- StaticRoute
- StaticNetMask

Other parameters that are normally supplied by DHCP may be provided statically by configuring their values. These parameters are:

- DNS1IP
- DNS2IP
- NTPIP
- AltNTPIP
- Domain

This completes the parameter settings you need to configure in order for the Cisco ATA to contact the TFTP server (without using DHCP) that will contain the configuration file for the Cisco ATA.

Voice Configuration Menu

The main reasons to use the voice configuration menu are to establish IP connectivity for the Cisco ATA if a DHCP server is not being used in your network environment, and to reset the Cisco ATA to its factory values if necessary. You can also use the voice configuration menu if you need to configure a small number of parameters or if the web interface and TFTP configuration are not available.

**Note**

Do not use the voice configuration menu to attempt to change any values that you configured by means of the TFTP configuration file method. Whenever the Cisco ATA refreshes, it downloads its ata<macaddress> configuration file or atadefault.cfg default configuration file from the TFTP server, and the values in either of these files will overwrite the values of any corresponding parameters configured with the voice configuration menu.

See [Chapter 5, “Parameters and Defaults,”](#) for a complete list of parameters and their definitions. Also see [Table 4-4 on page 4-12](#) for an alphabetical listing of configurable features and references to their corresponding parameters.

This section contains the following topics:

- [Using the Voice Configuration Menu, page 3-16](#)
- [Entering Alphanumeric Values, page 3-17](#)
- [Resetting the Cisco ATA to Factory Default Values, page 3-18](#)

Using the Voice Configuration Menu

To manually configure the Cisco ATA by using the voice configuration menu and the telephone keypad, perform the following steps:

Procedure

-
- Step 1** Connect an analog touch-tone phone to the port labeled **Phone 1** on the back of the Cisco ATA.
- Step 2** Lift the handset and press the function button located on the top of the Cisco ATA. You should receive the initial voice configuration menu voice prompt.
- Step 3** Using the telephone keypad, enter the voice menu code for the parameter that you want to configure or the command that you want to execute, then press #. For a list of voice menu codes, see [Appendix B, “Voice Menu Codes.”](#)

[Table 3-5](#) lists the menu options that you need to configure basic IP connectivity for the Cisco ATA, after which you can use the Cisco ATA web configuration page to configure additional parameters.



Note If you are using the voice configuration menu to statically configure the Cisco ATA IP address, you must disable DHCP by setting its value to 0.

Table 3-5 Parameters that Provide Basic IP Connectivity for the Cisco ATA

Voice Menu Number	Features
1	StaticIP—IP address of the Cisco ATA.
2	StaticRoute—Default gateway for the Cisco ATA to use.
10	StaticNetMask—Subnet mask of the Cisco ATA.
20	DHCP—Set value to 0 to disable the use of a DHCP server; set value to 1 to enable DHCP.
21	Review the IP address of the Cisco ATA.
22	Review the default router for the Cisco ATA to use.
23	Review subnet mask of the Cisco ATA.

- Step 4** Follow the voice prompts and enter the appropriate values, then press the # key.



Note Use the * key to indicate a delimiter (dot). For example, to enter an IP address of 192.168.3.1, you would enter 192*168*3*1 on your telephone keypad.



Note When entering values for a field that contains a hexadecimal value, you must convert the hexadecimal value to a decimal value in order to enter it into the voice configuration menu system. For example, to enter the hexadecimal value 0x6A, you would enter the number 106 on the telephone keypad.

The voice configuration menu repeats the value you entered, then prompts you to press one of the following keys:

- 1=Change your entered value
- 2=Review your entered value
- 3=Save your entered value
- 4=Review the current saved value

- Step 5** Press the # key after you have entered the desired key. If you do not press the # key, the system will automatically timeout after 10 seconds.
- Step 6** Cisco strongly recommends that you set a password. Use the voice menu code 7387277 (SETPASS) to configure a password through the voice configuration menu, after which you are prompted for the password whenever you attempt to change a parameter value.
- Step 7** After completing the configuration through the voice configuration menu, press the # key to exit.
- Step 8** Hang up the telephone. The Cisco ATA configuration refreshes. The function button fast-blinks when the refresh completes.

Entering Alphanumeric Values

Some voice configuration menu options require you to enter alphanumeric characters. Alphanumeric entry differs from numeric entry because you must press # after each character selected.

If you need to enter an alphanumeric value, the voice prompt tells you to enter an alphanumeric value; otherwise, enter a numeric value (0 to 9).

Table 3-6 lists the keys on a telephone keypad and their respective alphanumeric characters.

Using Table 3-6 as a guide, enter the appropriate number key on the telephone keypad as many times as needed to select the number, letter, or symbol required. For example, to enter 58sQ, you would enter:

```
5 # 8 # 7 7 7 7 7 # 7 7 7 7 7 7 7 # #
```

Table 3-6 Alphanumeric Characters

Key	Alphanumeric Characters
1	1 ./_ \ @ *space return + - ! , ? ~ ^ # = \$ % < > [] ; : { } () &
2	2 a b c A B C
3	3 d e f D E F
4	4 g h i G H I
5	5 j k l J K L
6	6 m n o M N O
7	7 p q r s P Q R S
8	8 t u v T U V
9	9 w x y z W X Y Z
0	0

Resetting the Cisco ATA to Factory Default Values

It is possible that you may, under some circumstances, want to reset the Cisco ATA to its factory default values. For example, this is the only way to recover a forgotten password without contacting your Cisco representative.

To perform a factory reset, you must use the voice configuration menu and follow these steps:

Procedure

- Step 1** Press the function button on the Cisco ATA.
 - Step 2** Press the digits **322873738 (FACTRESET)** then press **#** on your telephone keypad.
 - Step 3** Press **3** on your telephone keypad to confirm that you want to reset the Cisco ATA, then hang up the phone.
-

Cisco ATA Web Configuration Page

You can use the Cisco ATA web configuration page in a non-TFTP configuration environment, or in a TFTP configuration environment as a read-only record of individual customer parameters.

You can display the most recent Cisco ATA configuration file from the TFTP server by opening your web browser and typing the following:

http://<ipaddress>/refresh

where *ipaddress* is the IP address of the Cisco ATA.

[Figure 3-1](#) shows an example of the Cisco ATA web configuration page, which displays all configurable parameters.



Note

Do not use the web configuration page to attempt to change any values that you configured by means of the TFTP configuration file method. Whenever the Cisco ATA refreshes, it downloads its `ata<macaddress>` configuration file or `atadefault.cfg` default configuration file from the TFTP server, and the values in either of these files will overwrite the values of any corresponding parameters configured with the web configuration method.

You can access the web configuration page from any graphics-capable browser, such as Microsoft Internet Explorer or Netscape. This provides easy initial access to the Cisco ATA configuration within the administrator's private network.

Follow these steps to set parameters using the web configuration page:

Procedure

Step 1 Make sure that your PC and the Cisco ATA are already networked and visible to each another.

Step 2 Open your web browser.

Step 3 Enter the URL for your configuration page. The default URL for the web server is:

`http://IP Address/dev`

For example, the configuration page for a Cisco ATA with the IP address 192.168.3.225 is:

`http://192.168.3.225/dev`

Step 4 Select the values for the items that you want to configure. See [Chapter 5, "Parameters and Defaults,"](#) for a complete list of parameters and their definitions. Also see [Table 4-4 on page 4-12](#) for an alphabetical listing of configurable features and references to their corresponding parameters.



Note

Cisco strongly recommends that you set a password. Use the UIPassword parameter to configure a password, after which you are prompted for the password whenever you attempt to change a parameter value. Configuration parameters cannot be accessed through the voice configuration menu if the password contains one or more letters and can be changed only by using the web interface or the TFTP configuration method.

Step 5 Click **apply** to save your changes.

The Cisco ATA automatically refreshes its configuration.

Step 6 Close your web browser.

Web Interface Access-Control Configuration

To prevent tampering and unauthorized access to the Cisco ATA configuration, the Cisco ATA built-in web server can be disabled by using the OpFlags parameter.

Related Parameter

[OpFlags, page 5-33](#)—Bit 7

Refreshing or Resetting the Cisco ATA

Whenever you make configuration changes to your Cisco ATA configuration file, you can refresh or reset the Cisco ATA for these configuration changes to immediately take effect. If you do not refresh or reset the Cisco ATA, the configuration changes will take effect the next time the Cisco ATA contacts the TFTP server, which occurs based on the configured value of the CfgInterval parameter (see the ["Configuring the Cisco ATA Refresh Interval" section on page 4-9](#)).

**Note**

A refresh procedure will update the Cisco ATA configuration file. A reset procedure will also update the Cisco ATA configuration file, and will additionally power-down and power-up the Cisco ATA. A reset should not be necessary if your only goal is to update the configuration file.

HTTP Procedure to Refresh the Cisco ATA

To refresh the Cisco ATA, enter the following command from your web browser:

```
http://<ipaddress>/refresh
```

where *ipaddress* is the IP address of the Cisco ATA that you are refreshing.

HTTP Procedure to Reset the Cisco ATA

To reset the Cisco ATA, enter the following command from your web browser:

```
http://<ipaddress>/reset
```

where *ipaddress* is the IP address of the Cisco ATA that you are resetting.

HTTP Refresh and Reset Access-Control Configuration

You can configure the Cisco ATA to disable the use of the `http://ip/refresh` command that forces a configuration-file update. Use Bit 8 of the `OpFlags` parameter to control this refresh access.

You can also configure the Cisco ATA to disable the use of the `http://ip/reset` command that resets the Cisco ATA. Use Bit 9 of the `OpFlags` parameter to control this reset access.

Related Configuration Parameter

[OpFlags, page 5-33](#)

Upgrading the H.323 Signaling Image

For instructions on how to upgrade the Cisco ATA to the most recent H.323 signaling image, refer to the following list:

- To use the recommended TFTP method of upgrading the Cisco ATA, see the [“Upgrading the Signaling Image from a TFTP Server”](#) section on page 8-1.
- In the rare instance that you are not using the TFTP server to configure the Cisco ATA and to obtain software upgrades, you must manually upgrade to the latest signaling image immediately after the Cisco ATA boots up. In this case, see the [“Upgrading the Signaling Image Manually”](#) section on page 8-2.

