



Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide (SIP)

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-3410-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)

Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide (SIP)

Copyright © 2003, Cisco Systems, Inc.

All rights reserved.



Preface xi

Overview	xi
Audience	xi
Organization	xii
Conventions	xii
Related Documentation	xiv
Obtaining Documentation	xv
World Wide Web	xv
Documentation CD-ROM	xv
Ordering Documentation	xv
Documentation Feedback	xv
Obtaining Technical Assistance	xvi
Cisco.com	xvi
Technical Assistance Center	xvi
Cisco TAC Web Site	xvii
Cisco TAC Escalation Center	xvii

Cisco Analog Telephone Adaptor Overview 1-1

Session Initiation Protocol (SIP) Overview	1-2
SIP Capabilities	1-3
Components of SIP	1-3
SIP Clients	1-4
SIP Servers	1-4
Hardware Overview	1-5
Software Features	1-7
Voice Codecs Supported	1-7
Additional Supported Signaling Protocols	1-8
Other Supported Protocols	1-8
Cisco ATA SIP Services	1-8
Fax Services	1-9
Methods Supported	1-9
Supplementary Services	1-10
Installation and Configuration Overview	1-10

Installing the Cisco ATA 2-1

- Network Requirements 2-2
- Safety Recommendations 2-2
- What the Cisco ATA Package Includes 2-2
- What You Need 2-3
- Installation Procedure 2-3
- Power-Down Procedure 2-6

Configuring the Cisco ATA for SIP 3-1

- Default Boot Load Behavior 3-2
- Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation 3-3
- Steps Needed to Configure the Cisco ATA 3-5
 - Basic Configuration Steps in a TFTP Server Environment 3-5
 - Basic Configuration Steps in a Non-TFTP Server Environment 3-6
- Configuring the Cisco ATA Using a TFTP Server 3-7
 - Setting Up the TFTP Server with Cisco ATA Software 3-7
 - Configurable Features and Related Parameters 3-7
 - Creating Unique and Common Cisco ATA Configuration Files 3-8
 - Using ataname.exe Tool to Obtain MAC Address 3-10
 - Using the EncryptKey Parameter and cfgfmt Tool 3-11
 - atadefault.cfg Configuration File 3-12
 - Configuring the Cisco ATA to Obtain its Configuration File from the TFTP Server 3-13
 - Using a DHCP Server 3-13
 - Without Using a DHCP Server 3-15
- Voice Configuration Menu 3-15
 - Using the Voice Configuration Menu 3-16
 - Entering Alphanumeric Values 3-17
 - Resetting the Cisco ATA to Factory Default Values 3-18
- Cisco ATA Web Configuration Page 3-18
- Refreshing or Resetting the Cisco ATA 3-21
 - Procedure to Refresh the Cisco ATA 3-22
 - Procedure to Reset the Cisco ATA 3-22
- Upgrading the SIP Signaling Image 3-22

Basic and Additional SIP Services 4-1

- Important Basic SIP Services 4-1
 - Required Parameters 4-1

Establishing Authentication	4-2
Setting the Codec	4-3
Configuring Refresh Interval	4-3
Additional SIP Services	4-3
Advanced Audio Configuration	4-4
Billable Features	4-4
Comfort Noise During Silence Period When Using G.711	4-5
Configurable Hook Flash Timing	4-5
Configurable Mixing of Call Waiting Tone and Audio	4-5
Configurable On-hook delay	4-5
Debugging Diagnostics	4-5
Dial Plan	4-6
Disabling Access To The Web Interface	4-6
Distinctive Ringing	4-6
DNS SRV Support	4-6
Hardware Information Display	4-7
NAT Gateway	4-7
NAT/PAT Translation	4-7
Network Timing	4-8
OutBoundProxy Support	4-8
Progress Tones	4-8
Receiver-tagged VIA header	4-9
Repeat Dialing on Busy Signal	4-9
SIP Proxy Server Redundancy	4-10
Stuttering Dial Tone on Unconditional Call Forward	4-10
User Configurable Call Waiting Permanent Default Setting	4-10
User Configurable Timeout On No Answer for Call Forwarding	4-10
Setting Up and Placing a Call Without Using a SIP Proxy	4-11
Configuration	4-11
Placing an IP Call	4-12
Complete Reference Table of all Cisco ATA SIP Services	4-12
Parameters and Defaults	5-1
Configuration Text File Template	5-2
User Interface (UI) Parameter	5-3
UIPassword	5-3
Configuration Parameter	5-4
ToConfig	5-4

Parameters for Configuration Method **5-4**

UseTFTP **5-4**

TftpURL **5-5**

CfgInterval **5-5**

EncryptKey **5-6**

Network Parameters **5-6**

DHCP **5-7**

StaticIp **5-7**

StaticRoute **5-7**

StaticNetMask **5-8**

Account Information Parameters **5-8**

UID0 **5-9**

PWD0 **5-9**

UID1 **5-9**

PWD1 **5-10**

GkOrProxy **5-10**

Gateway **5-11**

Gateway2 **5-11**

UseLoginID **5-11**

LoginID0 **5-12**

LoginID1 **5-12**

Backup Server Parameters **5-13**

AltGk **5-13**

AltGkTimeOut **5-13**

GkTimeToLive **5-14**

GkId **5-14**

SIP Parameters **5-14**

UseSIP **5-14**

SIPRegInterval **5-15**

MAXRedirect **5-15**

SIPRegOn **5-16**

NATIP **5-16**

SIPPort **5-17**

MediaPort **5-17**

OutBoundProxy **5-17**

NatServer **5-18**

NatTimer **5-19**

Operating Parameters **5-19**

LBRCCodec	5-20
AudioMode	5-20
RxCodec	5-21
TxCodec	5-22
NumTxFrames	5-22
CallFeatures	5-23
PaidFeatures	5-24
CallerIdMethod	5-25
FeatureTimer	5-26
Polarity	5-27
ConnectMode	5-28
AutMethod	5-30
TimeZone	5-30
NTPIP	5-30
AltNTPIP	5-31
DNS1IP	5-31
DNS2IP	5-31
UDPTOS	5-32
SigTimer	5-32
OpFlags	5-34
VLANSetting	5-35
Optional Feature Parameters	5-35
NPrintf	5-36
TraceFlags	5-36
RingOnOffTime	5-37
IPDialPlan	5-38
DialPlan	5-38
About Dial Plan Commands	5-39
Dial Plan Blocking (In Rule)	5-41
'H' Rule to Support Hot/Warm Line	5-41
'P' Rule to Support Dial Prefix	5-42
Call-Progress Tone Parameters	5-42
List of Call-Progress Tone Parameters	5-42
Tone Parameter Syntax	5-42
How to Calculate Scaling Factors	5-43
Recommended Values	5-44
Specific Call-Progress Tone Parameter Information	5-44
CallCmd	5-47

Call Commands 6-1

- Call Command Structure 6-1
- Syntax 6-2
 - Context-Identifiers 6-3
 - Input Sequence Identifiers 6-4
 - Action Identifiers 6-4
- Call Command Example 6-5
- Call Command Behavior 6-7

Configuring and Debugging Fax Services 7-1

- Using Fax Pass-through Mode 7-1
 - Configuring the Cisco ATA for Fax Pass-through mode 7-2
 - AudioMode 7-2
 - ConnectMode 7-3
 - Configuring Cisco IOS Gateways to Enable Fax Pass-through 7-3
 - Enable Fax Pass-through Mode 7-4
 - Disable Fax Relay Feature 7-5
- Using FAX Mode 7-6
 - Configuring the Cisco ATA for Fax Mode 7-6
 - Configuring the Cisco ATA for Fax Mode on a Per-Call Basis 7-7
 - Configuring the Cisco IOS Gateway for Fax Mode 7-7
- Debugging the Cisco ATA 186/188 Fax Services 7-7
 - Common Problems When Using IOS Gateways 7-7
 - Using prserv for Diagnosing Fax Problems 7-9
 - prserv Overview 7-9
 - Analyzing prserv Output for Fax Sessions 7-9
 - Using rtpcatch for Diagnosing Fax Problems 7-12
 - rtpcatch Overview 7-12
 - Example of rtpcatch 7-13
 - Analyzing rtpcatch Output for Fax Sessions 7-16
 - Using rtpcatch to Analyze Common Causes of Failure 7-17
 - rtpcatch Limitations 7-19

Upgrading the Cisco ATA Signaling Image 8-1

- Upgrading the Signaling Image from a TFTP Server 8-1
- Upgrading the Signaling Image Manually 8-2
 - Preliminary Steps 8-3

Running the Executable File	8-3
Upgrade Requirements	8-3
Syntax	8-3
Upgrade Procedure	8-4
Confirming a Successful Signaling Image Upgrade	8-5
Using a Web Browser	8-5
Using the Voice Configuration Menu	8-5
Troubleshooting	9-1
General Troubleshooting Tips	9-1
Symptoms and Actions	9-2
Installation and Upgrade Issues	9-3
Debugging	9-4
Frequently Asked Questions	9-5
Contacting TAC	9-6
Using SIP Supplementary Services	A-1
Changing Call Commands	A-1
Cancelling a Supplementary Service	A-1
Common Supplementary Services	A-1
Caller ID	A-2
Call-Waiting Caller ID	A-2
Voice Mail Indication	A-2
Unattended Transfer	A-3
Semi-unattended Transfer	A-3
Fully Unattended Transfer	A-3
Attended Transfer	A-4
Making a Conference Call in the United States	A-4
Making a Conference Call in Sweden	A-4
Call Waiting in the United States	A-5
Call Waiting in Sweden	A-5
About Call Forwarding	A-5
Call Forwarding in the United States	A-5
Call Forwarding in Sweden	A-6
Call Return in the United States	A-6
Call Return in Sweden	A-6

Calling Line Identification Presentation	A-6
About Calling Line Identification Restriction	A-6
Calling Line Identification Restriction in the United States	A-7
Calling Line Identification Restriction in Sweden	A-7

Voice Menu Codes B-1

Cisco ATA Specifications C-1

Physical Specifications	C-1
Electrical Specifications	C-2
Environmental Specifications	C-2
Immunity Specifications	C-2
Physical Interfaces	C-3
Ringing Characteristics	C-3
Software Specifications	C-3
SIP Compliance Reference Information	C-5

SIP Call Flows D-1

Supported SIP Request Methods	D-1
Call Flow Scenarios for Successful Calls	D-2
Cisco ATA-to-SIP Server—Registration without Authentication	D-2
Cisco ATA-to-SIP Server—Registration with Authentication	D-3
Cisco ATA-to-Cisco ATA—Basic SIP to SIP Call without Authentication	D-6
Cisco ATA-to-Cisco ATA—Basic SIP to SIP Call with Authentication	D-12

GLOSSARY

INDEX



Preface

This preface includes the following sections:

- Overview, page xi
- Audience, page xi
- Organization, page xii
- Conventions, page xii
- Related Documentation, page xiv
- Obtaining Documentation, page xv
- Obtaining Technical Assistance, page xvi

Overview

The *Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide (SIP)* provides the information you need to install, configure and manage the Cisco ATA 186 and Cisco ATA 188 on a Session Initiation Protocol (SIP) network.



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.

Audience

This guide is intended for service providers and network administrators who administer Voice over IP (VoIP) services using the Cisco ATA. Most of the tasks described in this guide are not intended for end users of the Cisco ATA. Many of these tasks impact the ability of the Cisco ATA to function on the network, and require an understanding of IP networking and telephony concepts.

Organization

Table 1 provides an overview of the organization of this guide.

Table 1 *Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide (SIP) Organization*

Chapter	Description
Chapter 1, "Cisco Analog Telephone Adaptor Overview"	Provides descriptions of hardware and software features of the Cisco ATA Analog Telephone Adaptor along with a brief overview of the Session Initiation Protocol (SIP).
Chapter 2, "Installing the Cisco ATA"	Provides information about installing the Cisco ATA.
Chapter 3, "Configuring the Cisco ATA for SIP"	Provides information about configuring the Cisco ATA and the various methods for configuration.
Chapter 4, "Basic and Additional SIP Services"	Provides information about SIP services that the Cisco ATA supports.
Chapter 5, "Parameters and Defaults,"	Provides information on all parameters and defaults that you can use to configure the Cisco ATA.
Chapter 6, "Call Commands"	Provides the Cisco ATA call commands for SIP.
Chapter 7, "Configuring and Debugging Fax Services"	Provides instructions for configuring both ports of the Cisco ATA to support fax transmission.
Chapter 8, "Upgrading the Cisco ATA Signaling Image"	Provides instructions for remotely upgrading Cisco ATA software.
Chapter 9, "Troubleshooting"	Provides basic testing and troubleshooting procedures for the Cisco ATA.
Appendix A, "Using SIP Supplementary Services"	Provides end-user information about pre-call and mid-call services.
Appendix B, "Voice Menu Codes"	Provides a quick-reference list of the voice configuration menu options for the Cisco ATA.
Appendix C, "Cisco ATA Specifications"	Provides physical specifications for the Cisco ATA.
Appendix D, "SIP Call Flows"	Provides Cisco ATA call flows for SIP scenarios.
Glossary	Provides definitions of commonly used terms.
Index	Provides reference information.

Conventions

This document uses the following conventions:

- Alternative keywords are grouped in braces and separated by vertical bars (for example, {**x** | **y** | **z**}).
- Arguments for which you supply values are in *italic* font.
- Commands and keywords are in **boldface** font.
- Elements in square brackets ([]) are optional.
- Information you must enter is in **boldface screen** font.
- Optional alternative keywords are grouped in brackets and separated by vertical bars (for example, [**x** | **y** | **z**]).

- Terminal sessions and information the system displays are in `screen` font.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Tip**

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Warning**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix “Translated Safety Warnings.”)

Waarschuwing

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel “Translated Safety Warnings” (Vertalingen van veiligheidsvoorschriften) raadplegen.)

Varoitus

Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä “Translated Safety Warnings” (käännetyt turvallisuutta koskevat varoitukset).)

Attention

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).

Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körpverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)
Avvertenza	Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).
Advarsel	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").
¡Advertencia!	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
Varning!	Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

Related Documentation

- RFC3261 (*SIP: Session Initiation Protocol*)
- RFC2543 (*SIP: Session Initiation Protocol*)
- *Cisco ATA SIP Compliance Reference Information*
<http://www-vnt.cisco.com/SPUniv/SIP/documents/CiscoATASIPComplianceRef.pdf>
- RFC768 (*User Datagram Protocol*)
- RFC2198 (*RTP Payload for Redundant Audio Data*)
- RFC2833 (*RTP Payload for DTMF Digits, Telephony Phones and Telephony Signals*)
- RFC2327 (*SDP: Session Description Protocol*)
- RFC3266 (*Support for IPv6 in Session Description Protocol (SDP)*)

- *Read Me First - ATA Boot Load Information*
- *Cisco ATA 186 and Cisco 188 Analog Telephone Adaptor At a Glance*
- *Regulatory Compliance and Safety Information for the Cisco ATA 186 and Cisco 188*
- *Cisco ATA Release Notes*

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com>

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products Marketplace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

<http://www.cisco.com/register/>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.



Cisco Analog Telephone Adaptor Overview

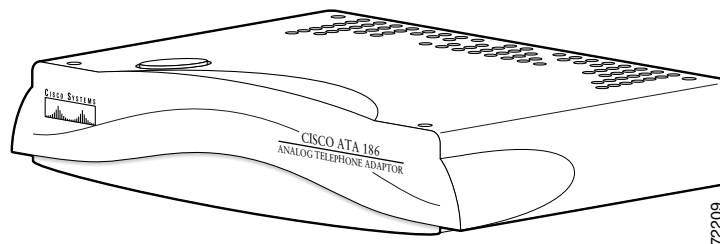
This section describes the hardware and software features of the Cisco Analog Telephone Adaptor (Cisco ATA) and includes a brief overview of the Session Initiation Protocol (SIP).

The Cisco ATA analog telephone adaptors are handset-to-Ethernet adaptors that allow regular analog telephones to operate on IP-based telephony networks. Cisco ATAs support two voice ports, each with an independent telephone number. The Cisco ATA 188 also has an RJ-45 10/100BASE-T data port.

This section covers the following topics:

- Session Initiation Protocol (SIP) Overview, page 1-2
- Hardware Overview, page 1-5
- Software Features, page 1-7
- Installation and Configuration Overview, page 1-10

Figure 1-1 Cisco ATA Analog Telephone Adaptor



The Cisco ATA, which operates with Cisco voice-packet gateways, makes use of broadband pipes that are deployed through a digital subscriber line (DSL), fixed wireless-cable modem, and other Ethernet connections.



Note

The term *Cisco ATA* refers to both the Cisco ATA 186 and the Cisco ATA 188, unless otherwise stated.

Figure 1-2 Cisco ATA 186 as Endpoint in SIP Network

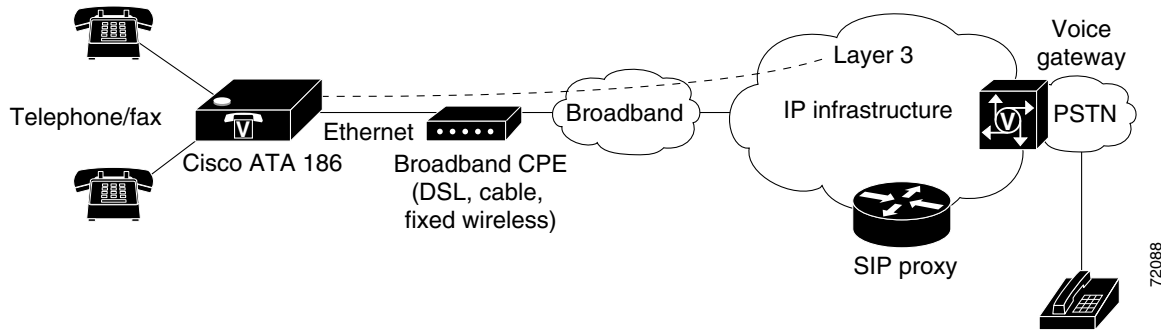
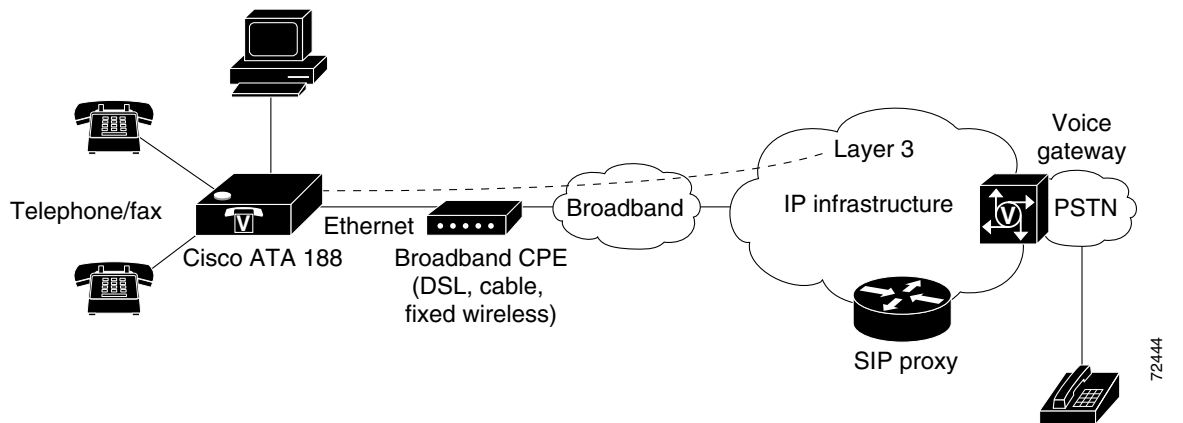


Figure 1-3 Cisco ATA 188 as Endpoint in SIP Network



Session Initiation Protocol (SIP) Overview

Session Initiation Protocol (SIP) is the Internet Engineering Task Force (IETF) standard for real-time calls and conferencing over Internet Protocol (IP). SIP is an ASCII-based, application-layer control protocol (defined in RFC3261) that can be used to establish, maintain, and terminate multimedia sessions or calls between two or more endpoints.

Like other Voice over IP (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.



Note

SIP for the Cisco ATA is compliant with RFC2543.

This section contains the following topics:

- SIP Capabilities, page 1-3
- Components of SIP, page 1-3

SIP Capabilities

SIP provides the following capabilities:

- Determines the availability of the target endpoint. If a call cannot be completed because the target endpoint is unavailable, SIP determines whether the called party is already on the phone or did not answer in the allotted number of rings. SIP then returns a message indicating why the target endpoint was unavailable.
- Determines the location of the target endpoint. SIP supports address resolution, name mapping, and call redirection.
- Determines the media capabilities of the target endpoint. Using the Session Description Protocol (SDP), SIP determines the lowest level of common services between endpoints. Conferences are established using only the media capabilities that are supported by all endpoints.
- Establishes a session between the originating and target endpoint. If the call can be completed, SIP establishes a session between the endpoints. SIP also supports mid-call changes, such as adding another endpoint to the conference or changing the media characteristic or codec.
- Handles the transfer and termination of calls. SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP establishes a session between the transferee and a new endpoint (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties. Conferences can consist of two or more users and can be established using multicast or multiple unicast sessions.

Components of SIP

SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can function in one of the following roles:

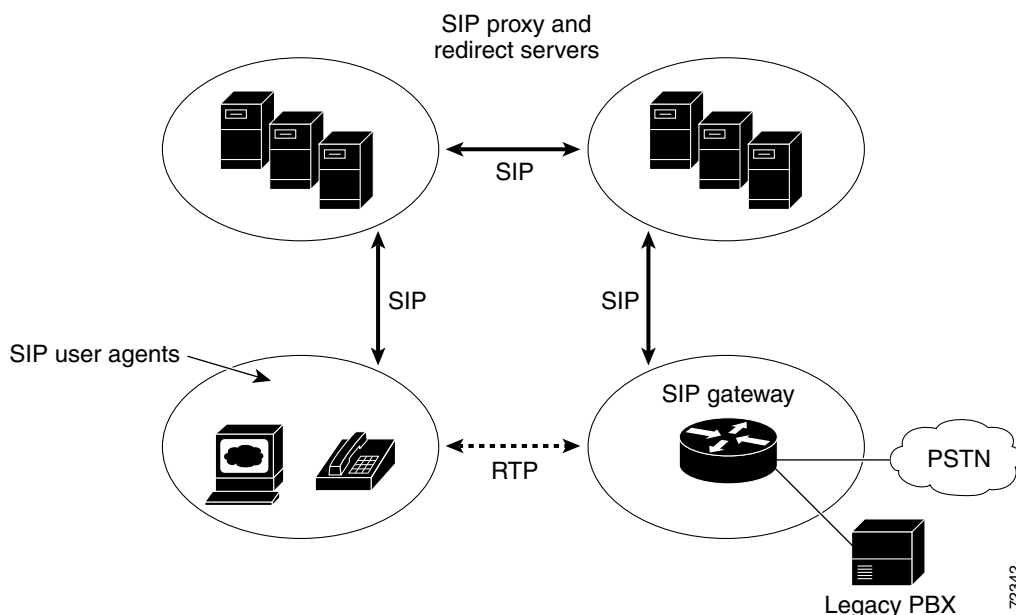
- User agent client (UAC)—A client application that initiates the SIP request.
- User agent server (UAS)—A server application that contacts the user when a SIP request is received and returns a response on behalf of the user.

Typically, a SIP endpoint is capable of functioning as both a UAC and a UAS, but functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiated the request.

From an architectural standpoint, the physical components of a SIP network can also be grouped into two categories—Clients and servers. Figure 1-4 illustrates the architecture of a SIP network.

**Note**

SIP servers can interact with other application services, such as Lightweight Directory Access Protocol (LDAP) servers, a database application, or an extensible markup language (XML) application. These application services provide back-end services such as directory, authentication, and billable services.

Figure 1-4 SIP Architecture

SIP Clients

SIP clients include:

- Gateways—Provide call control. Gateways provide many services, the most common being a translation function between SIP conferencing endpoints and other terminal types. This function includes translation between transmission formats and between communications procedures. In addition, the gateway also translates between audio and video codecs and performs call setup and clearing on both the LAN side and the switched-circuit network side.
- Telephones—Can act as either a UAS or UAC. The Cisco ATA can initiate SIP requests and respond to requests.

SIP Servers

SIP servers include:

- Proxy server—The proxy server is an intermediate device that receives SIP requests from a client and then forwards the requests on the client's behalf. Proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
- Redirect server—Receives SIP requests, strips out the address in the request, checks its address tables for any other addresses that may be mapped to the address in the request, and then returns the results of the address mapping to the client. Redirect servers provide the client with information about the next hop or hops that a message should take, then the client contacts the next hop server or UAS directly.
- Registrar server—Processes requests from UACs for registration of their current location. Registrar servers are often co-located with a redirect or proxy server.

Hardware Overview

The Cisco ATA 186 and Cisco ATA 188 are compact, easy to install devices. Figure 1-5 shows the rear panel of the Cisco ATA 186. Figure 1-6 shows the rear panel of the Cisco ATA 188.

Figure 1-5 Cisco ATA 186—Rear View

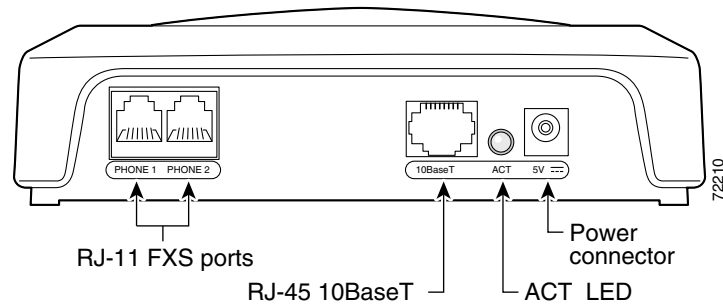
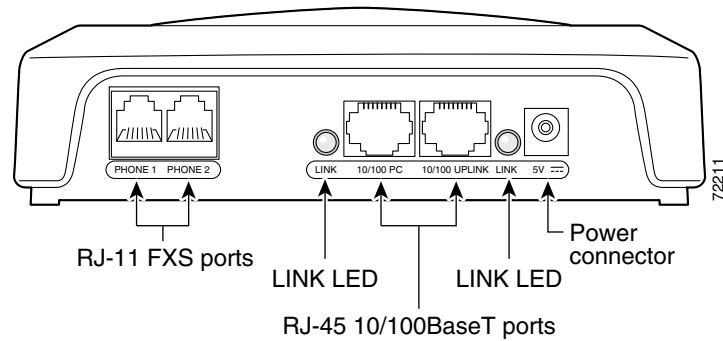


Figure 1-6 Cisco ATA 188—Rear View



The unit provides the following connectors and indicators:

- 5V power connector.
- Two RJ-11 FXS (Foreign Exchange Station) ports—The Cisco ATA supports two independent RJ-11 telephone ports that can connect to any standard analog telephone device. Each port supports either voice calls or fax sessions, and both ports can be used simultaneously.

**Note**

The Cisco ATA186-I1 and Cisco ATA188-I1 provide 600-ohm resistive impedance. The Cisco ATA186-I2 and Cisco ATA188-I2 provide 270 ohm + 750 ohm // 150-nF complex impedance. The impedance option is requested when you place your order and should match your specific application. If you are not sure of the applicable configuration, check your country or regional telephone impedance requirements.

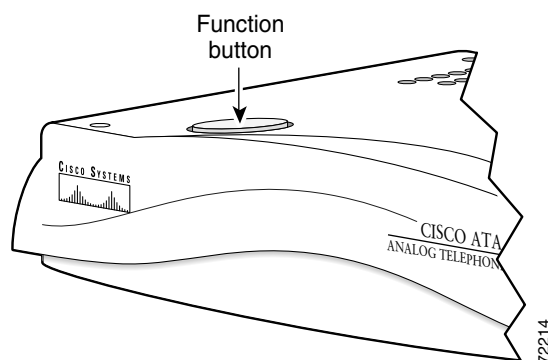
- Ethernet ports
 - The Cisco ATA 186 has one RJ-45 10BASE-T uplink Ethernet port to connect the Cisco ATA 186 to a 10/100BASE-T hub or another Ethernet device.
 - The Cisco ATA 188 has two Ethernet ports: an RJ-45 10/100BASE-T uplink port to connect the Cisco ATA 188 to a 10/100BASE-T hub or another Ethernet device and an RJ-45 10/100BASE-T data port to connect an Ethernet-capable device, such as a computer, to the network.

**Note**

The Cisco ATA 188 performs auto-negotiation for duplexity and speed and is capable of 10/100 Mbps, full-duplex operation. The Cisco ATA 186 is fixed at 10 Mbps, half-duplex operation.

- The Cisco ATA 188 RJ-45 LED shows network link and activity. The LED blinks twice when the Cisco ATA is first powered on, then turns off if there is no link or activity. The LED blinks to show network activity and is solid when there is a link.
- The Cisco ATA 186 RJ-45 LED is solid when the Cisco ATA is powered on and blinks to show network activity.
- Function button—The function button is located on the top panel of the unit (see Figure 1-7).

Figure 1-7 Function Button



The function button lights when you pick up the handset of a telephone attached to the Cisco ATA. The button blinks quickly when the Cisco ATA is upgrading its configuration.

**Note**

If the function button blinks slowly, the Cisco ATA cannot find the DHCP server. Check your Ethernet connections and make sure the DHCP server is available.

Pressing the function button allows you to access to the voice configuration menu. For additional information about the voice configuration menu, see the “Voice Configuration Menu” section on page 3-15.

**Caution**

Never press the function button during an upgrade process. Doing so may interfere with the process and may permanently disable the Cisco ATA.

Software Features

The Cisco ATA supports the following protocols, services and methods:

- Voice Codecs Supported, page 1-7
- Additional Supported Signaling Protocols, page 1-8
- Other Supported Protocols, page 1-8
- Cisco ATA SIP Services, page 1-8
- Fax Services, page 1-9
- Methods Supported, page 1-9
- Supplementary Services, page 1-10

Voice Codecs Supported

The Cisco ATA supports the following voice codecs (check your other network devices for the codecs they support):

- G.711μ-law
- G.711A-law
- G.723.1
- G.729
- G.729A
- G.729B
- G.729AB

Additional Supported Signaling Protocols

In addition to SIP, the Cisco ATA supports the following signaling protocols:

- H.323
- Skinny Client Control Protocol (SCCP)
- Media Gateway Control Protocol (MGCP)

SIP and H.323 share the same software image. SCCP and MGCP also share a software image, which is separate from the SIP/H.323 image. If you wish to perform a cross-protocol upgrade from SIP to another signaling image, see the “Upgrading the Signaling Image from a TFTP Server” section on page 8-1.

Other Supported Protocols

Other protocols that the Cisco ATA supports include the following:

- 802.1Q VLAN tagging
- Cisco Discovery Protocol (CDP)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Internet Control Message Protocol (ICMP)
- Internet Protocol (IP)
- Real-Time Transport Protocol (RTP)
- Transmission Control Protocol (TCP)
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)

Cisco ATA SIP Services

For a list of required SIP parameters as well as descriptions of all supported Cisco ATA SIP services and cross references to the parameters for configuring these services, see Chapter 4, “Basic and Additional SIP Services.”

These services include the following features:

- IP address assignment—DHCP-provided or statically configured
- Cisco ATA configuration by means of a TFTP server, web browser, or voice configuration menu.
- VLAN configuration
- Cisco Discovery Protocol (CDP)
- Low-bit-rate codec selection
- User authentication
- Configurable tones (dial tone, busy tone, alert tone, reorder tone, call waiting tone)
- Dial plans
- Network Address Translation (NAT) Gateway
- NAT/Port Address Translation (PAT) translation

- SIP proxy server redundancy
- Outbound-proxy support
- DNS SRV support
- User-configurable, call-waiting, permanent default setting
- Comfort noise during silence period when using G.711
- Advanced audio
- Billable features
- Caller ID format
- Ring cadence format
- Silence suppression
- Hook-flash detection timing configuration
- Configurable on-hook delay
- UDP Type of Service (ToS) configuration
- Debugging and diagnostic tools

Fax Services

The Cisco ATA supports two modes of fax services, in which fax signals are transmitted using the G.711 codec:

- Fax pass-through mode—Receiver-side Called Station Identification (CED) tone detection with automatic G.711A-law or G.711μ-law switching.
- Fax mode—The Cisco ATA is configured as a G.711-only device.

How you set Cisco ATA fax parameters depends on what network gateways are being used. You may need to modify the default fax parameter values (see Chapter 7, “Configuring and Debugging Fax Services”).

**Note**

Success of fax transmission depends on network conditions and fax modem response to these conditions. The network must have reasonably low network jitter, network delay, and packet loss rate.

Methods Supported

The Cisco ATA supports the methods listed below. For more information, refer to RFC3261 (*SIP: Session Initiation Protocol*).

- REGISTER
- INVITE
- BYE
- CANCEL

- NOTIFY
- OPTIONS
- ACK

Supplementary Services

SIP supplementary services are services that you can use to enhance your telephone service. For information on how to enable and subscribe to these services, see the “CallFeatures” section on page 5-23 and the “PaidFeatures” section on page 5-24.

For information on how to use these services, see Appendix A, “Using SIP Supplementary Services.”

The following list contains the SIP supplementary services that the Cisco ATA supports:

- Caller ID
- Call-waiting caller ID
- Voice mail indication
- Making a conference call
- Call waiting
- Call forwarding
- Call return
- Calling-line identification
- Unattended transfer
- Attended transfer

Installation and Configuration Overview

Table 1-1 provides the basic steps required to install and configure the Cisco ATA to make it operational in a typical SIP environment where a large number of Cisco ATAs must be deployed.

Table 1-1 Overview of the Steps Required to Install and Configure the Cisco ATA and Make it Operational

Action	Reference
1. Plan the network and Cisco ATA configuration.	
2. Install the Ethernet connection.	
3. Install and configure the other network devices.	
4. Install the Cisco ATA but do not power up the Cisco ATA yet.	What the Cisco ATA Package Includes, page 2-2
5. Download the desired Cisco ATA release software zip file from the Cisco web site, then configure the Cisco ATA.	Chapter 3, “Configuring the Cisco ATA for SIP”
6. Power up the Cisco ATA.	
7. Periodically, you can upgrade the Cisco ATA to a new signaling image by using the TFTP server-upgrade method or the manual-upgrade method.	Chapter 8, “Upgrading the Cisco ATA Signaling Image”



Installing the Cisco ATA

This section provides instructions for installing the Cisco ATA 186 and Cisco ATA 188. Before you perform the installation, be sure you have met the following prerequisites:

- Planned the network and Cisco ATA configuration.
- Installed the Ethernet connection.
- Installed and configured the other network devices.

This section contains the following topics:

- Network Requirements, page 2-2
- Safety Recommendations, page 2-2
- What the Cisco ATA Package Includes, page 2-2
- What You Need, page 2-3
- Installation Procedure, page 2-3
- Power-Down Procedure, page 2-6



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.

Network Requirements

The Cisco ATA acts as an endpoint on an IP telephony network. The following equipment is required:

- Call Control system
- Voice packet gateway—Required if you are connecting to the Public Switched Telephone Network (PSTN). A gateway is not required if an analog key system is in effect.
- Ethernet connection

Safety Recommendations

To ensure general safety, follow these guidelines:

- Do not get this product wet or pour liquids into this device.
- Do not open or disassemble this product.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Use only the power cube that comes with the Cisco ATA.



Warning

Ultimate disposal of this product should be handled according to all national laws and regulations.



Warning

Read the installation instructions before you connect the system to its power source.



Warning

The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.



Warning

Do not work on the system or connect or disconnect cables during periods of lightning activity.

For translated warnings, see the *Regulatory Compliance and Safety Information for the Cisco ATA 186 and Cisco ATA 188* manual.

What the Cisco ATA Package Includes

The Cisco ATA package contains the following items:

- Cisco ATA 186 or Cisco ATA 188 Analog Telephone Adaptor
- *Read Me First - ATA Boot Load Information*
- *Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor at a Glance*

- *Regulatory Compliance and Safety Information for the Cisco ATA 186 and Cisco ATA 188*
- 5V power adaptor
- Power cord

**Note**

The Cisco ATA is intended for use only with the 5V DC power adaptor that comes with the unit.

What You Need

You also need the following items:

- Category-3 10BASE-T or 100BASE-T or better Ethernet cable. One cable is needed for each Ethernet connection.

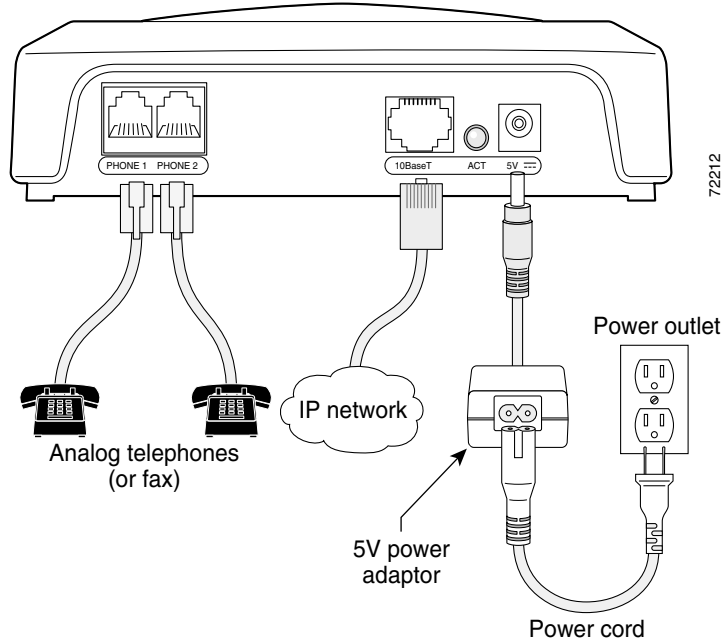
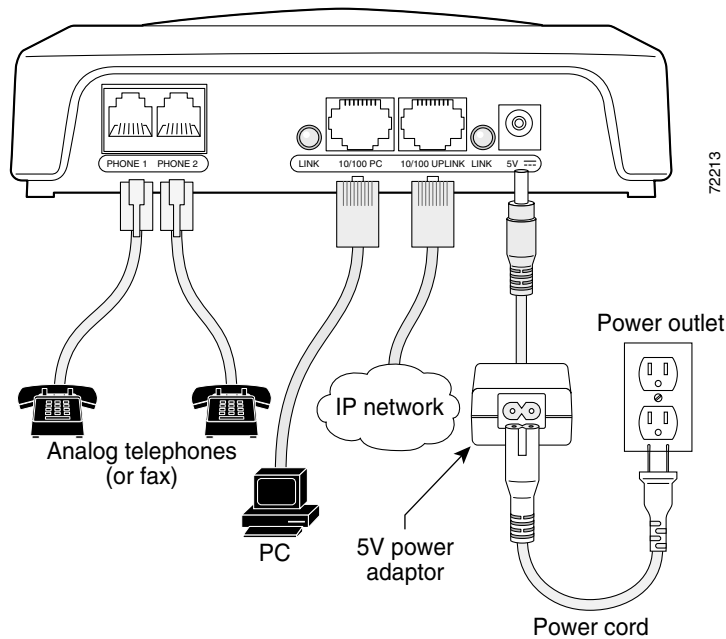
A Category-3 Ethernet cable supports 10BASE-T for up to 100 meters without quality degradation, and a Category-3 Ethernet cable supports 100BASE-T for up to 10 meters without quality degradation.

For uplink connections, use a crossover Ethernet cable to connect the Cisco ATA to another Ethernet device (such as a router or PC) without using a hub. Otherwise, use straight-through Ethernet cables for both uplink and data port connections.

- Access to an IP network
- One or two analog Touch-Tone telephones or fax machines, or one of each

Installation Procedure

After the equipment is in place, see Figure 2-1 (for Cisco ATA 186) or Figure 2-2 (for Cisco ATA 188) and follow the next procedure to install the Cisco ATA.

Figure 2-1 Cisco ATA 186 Rear Panel Connections**Figure 2-2 Cisco ATA 188 Rear Panel Connections****Procedure**

- Step 1** Place the Cisco ATA near an electrical power outlet.
- Step 2** Connect one end of a telephone line cord to the **Phone 1** input on the rear panel of the Cisco ATA. Connect the other end to an analog telephone set.

If you are connecting a telephone set that was previously connected to an active telephone line, unplug the telephone line cord from the wall jack and plug it into the **Phone 1** input.

**Warning**

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

**Caution**

Do not connect the **Phone** input ports to a telephone wall jack. To avoid damaging the Cisco ATA or telephone wiring in the building, do not connect the Cisco ATA to the telecommunications network. Connect the **Phone** port to a telephone only, never to a telephone wall jack.

**Note**

The telephone must be switched to tone setting (not pulse) for the Cisco ATA to operate properly.

Step 3

(Optional) Connect the telephone line cord of a second telephone to the **Phone 2** input port.

**Note**

If you are connecting only one telephone to the Cisco ATA, you must use the **Phone 1** input port.

Step 4

Connect an Ethernet cable to the uplink RJ-45 connector on the Cisco ATA. For the Cisco ATA 186, this is the 10BASE-T connector; for the Cisco ATA 188, this is the 10/100UPLINK connector.

**Note**

Use a crossover Ethernet cable to connect the Cisco ATA to another Ethernet device (such as a router or PC) without using a hub. Otherwise, use a straight-through Ethernet cable.

Step 5

(Cisco ATA 188 only—optional) Connect a straight-through Ethernet cable from your PC to the 10/100 PC RJ-45 connector on the Cisco ATA.

Step 6

Connect the socket end of the power cord to the 5V DC power adaptor.

Step 7

Insert the power adaptor cable into the power connector on the Cisco ATA.

**Warning**

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

Step 8

Connect the plug end of the 5V DC power adaptor cord into an electrical power outlet.

When the Cisco ATA is properly connected and powered up, the green activity LED flashes to indicate network activity. This LED is labeled **ACT** on the rear panel of the Cisco ATA 186 and is labeled **LINK** on the rear panel of the Cisco ATA 188.

**Caution**

Do not cover or block the air vents on either the top or the bottom surface of the Cisco ATA. Overheating can cause permanent damage to the unit.

For more information about LEDs and the function button, see the “Hardware Overview” section on page 1-5.

Power-Down Procedure

**Caution**

If you need to power down Cisco ATA 186 or Cisco 188 at any time, use the following power-down procedure to prevent damage to the unit.

Procedure

-
- Step 1** Unplug the RJ45 Ethernet cable
- Step 2** Wait for 20 seconds.
- Step 3** Unplug the power cable.
-



Configuring the Cisco ATA for SIP

This section describes how to configure the Cisco ATA to operate with the Session Initiation Protocol (SIP) signaling image and how the Cisco ATA obtains the latest signaling image.

You can configure the Cisco ATA for use with SIP 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.
- Refreshing or Resetting the Cisco ATA, page 3-21—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 SIP Signaling Image, page 3-22—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 bootload 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 bootload 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.

4. 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.

5. 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.
6. 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 that indicates 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 5-34
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 5-35

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 SIP 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” section on 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.	Configuring Refresh Interval, 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 3-13
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 3-21

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
<ol style="list-style-type: none"> 1. Download the desired Cisco ATA release software zip file from the Cisco web site: <ol style="list-style-type: none"> a. If you are a registered CCO user, go to the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/ata186 b. 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. c. Extract the files to the desired location on your PC. 	
 Note The file that contains the protocol signaling image has an extension of .zup.	
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 3-13

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. |
| <hr/> | |
| 
Note | The file that contains the protocol signaling image has an extension of .zup. |
| <hr/> | |
| 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 SIP parameters. These parameters must be properly configured for the Cisco ATA to work.

For descriptions of important Cisco ATA SIP services that you can configure, and references to their configuration parameters, see the “Important Basic SIP Services” section on page 4-1 and the “Additional SIP Services” section on page 4-3.

Table 4-3 on page 4-12 lists, in alphabetical order, various features that you can configure for the Cisco ATA. Table 4-3 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 1 to enable the SIP protocol. This parameter is 0 (for H.323) by default.

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 SIP parameters in the examples. See Chapter 4, “Basic and Additional SIP Services,” 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:1
```

**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 is 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.
- `output-binary-file` is the final output binary file that Cisco ATA uses as the TFTP configuration file.

Example

```
cfgfmt -tp tag.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. This example also uses a *ptag* file name of *ptag.dat*.

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 3-21.)

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 3-15

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 3-14

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 5-34).

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, **SIP**)
- 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 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 4-3 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.

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

Voice Menu Number	Features
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. The different colors on the screen are for different parameter groupings, as described in Chapter 5, “Parameters and Defaults.”

**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.

[illegible]

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 4-3 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.

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.



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.

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.

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.

Upgrading the SIP Signaling Image

For instructions on how to upgrade the Cisco ATA to the most recent SIP 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.



Basic and Additional SIP Services

This section provides information about key basic and additional SIP services that the Cisco ATA supports:

- Important Basic SIP Services, page 4-1—This section includes a list of parameters that you must configure in order for the Cisco ATA to function in a SIP environment.
- Additional SIP Services, page 4-3—This section contains information about additional, commonly used SIP features, with references to the parameters for configuring these services.
- Complete Reference Table of all Cisco ATA SIP Services, page 4-12—This section contains a complete listing of Cisco ATA services supported for SIP, and includes cross references to the parameters for configuring these services. This section includes services not described in the sections about the key basic SIP services and the commonly used additional SIP services.



Note

The term *Cisco ATA* refers to both the Cisco ATA 186 and the Cisco ATA 188, unless otherwise stated.

Important Basic SIP Services

This section provides descriptions and cross references for configuring required SIP parameters and also for configuring other important basic SIP services:

- Required Parameters, page 4-1
- Establishing Authentication, page 4-2
- Setting the Codec, page 4-3
- Configuring Refresh Interval, page 4-3

Required Parameters

If the UseSIP parameter is set to 1 (you are using the SIP protocol), you need to supply values for the required SIP parameters shown in Table 4-1. The Parameter column provides the name of the parameter and a cross reference which provides a more-detailed description of the parameter.



Note

See *Chapter 5, “Parameters and Defaults,”* for information about additional Cisco ATA parameters.

Table 4-1 Required SIP Parameters and Defaults

Parameter	Value Type	Description	Voice Menu Access Code	Minimum Value	Maximum Value	Default
SIPRegInterval, page 5-15	Integer	Seconds between registration renewal	203	1	86400	3600
MAXRedirect, page 5-15	Integer	Maximum number of times to try redirection	202	0	10	5
SIPRegOn, page 5-16	Integer	Enable SIP registration	204	0	1	0
NATIP, page 5-16	IP address	WAN address of the attached router/NAT; currently only used to support SIP behind a NAT.	200	0	255	0.0.0.0
SIPPort, page 5-17	Integer	Port to listen for incoming SIP requests	201	1	65535	5060
MediaPort, page 5-17	Integer	Base port to receive RTP media; only used to support SIP behind a NAT	202	1	65535	16384
OutBoundProxy, page 5-17	Alphanumeric string	Proxy server for all outbound SIP requests. All SIP requests are sent to OutBoundProxy, when configured, instead of to the configured GkOrProxy.	206	—	—	0
GkOrProxy, page 5-10	Alphanumeric string	SIP proxy server address or registrar address.	5	—	—	0
UseSIP, page 5-14	Boolean	Set to 1 for SIP mode.	38	—	—	0
ToConfig, page 5-4	Boolean	Set to 0 after you have completed configuration of the Cisco ATA. If this value remains at 1, the Cisco ATA will unnecessarily continue to contact the TFTP server.	80001	—	—	1

Establishing Authentication

The Cisco ATA supports two levels of authentication, depending on the setting of the UseLoginID parameter:

- If UseLoginID is set to 0, the user ID (UID0 or UID1) is used with a user-supplied password (PWD0 or PWD1) for authentication.
- If UseLoginID is set to 1, you must supply a login ID (LoginID0 or LoginID1) and a password (PWD0 or PWD1) for authentication.

Related Configuration Parameters

- UseLoginID, page 5-11
- UID0, page 5-9
- UID1, page 5-9

- LoginID0, page 5-12
- LoginID1, page 5-12
- PWD0, page 5-9
- PWD1, page 5-10

Setting the Codec

The LBRCodec (low-bit-rate codec) parameter determines whether the G.723 or G.729A codec, in addition to G.711A-law and G.711 μ -law, can be used for receiving and transmitting. For configuration information, see the “LBRCodec” section on page 5-20.

Configuring Refresh Interval

When the value specified in the CfgInterval parameter is reached, the Cisco ATA attempts to refresh its configuration file from the TFTP server. By opening a web page for the Cisco ATA, you can perform a refresh before the scheduled refresh. Set the CfgInterval parameter to an interval value (in seconds) for refreshing the Cisco ATA configuration file. Cisco recommends that the interval be semi-random to prevent many simultaneous contacts with the TFTP server. For more information, see the “CfgInterval” section on page 5-5.

When the Cisco ATA contacts the TFTP server, it also checks to see if an upgrade signaling image has been placed on the TFTP server. If such an image exists, the Cisco ATA will download this image.

Additional SIP Services

This section describes additional SIP services and, where applicable, provides configuration information and cross references to the parameters for configuring these services. These services are listed alphabetically.

- Advanced Audio Configuration, page 4-4
- Billable Features, page 4-4
- Comfort Noise During Silence Period When Using G.711, page 4-5
- Configurable Hook Flash Timing, page 4-5
- Configurable Mixing of Call Waiting Tone and Audio, page 4-5
- Configurable On-hook delay, page 4-5
- Debugging Diagnostics, page 4-5
- Dial Plan, page 4-6
- Disabling Access To The Web Interface, page 4-6
- Distinctive Ringing, page 4-6
- DNS SRV Support, page 4-6
- Hardware Information Display, page 4-7
- NAT Gateway, page 4-7
- NAT/PAT Translation, page 4-7

- Network Timing, page 4-8
- OutBoundProxy Support, page 4-8
- Progress Tones, page 4-8
- Receiver-tagged VIA header, page 4-9
- Repeat Dialing on Busy Signal, page 4-9
- SIP Proxy Server Redundancy, page 4-10
- Stuttering Dial Tone on Unconditional Call Forward, page 4-10
- User Configurable Call Waiting Permanent Default Setting, page 4-10
- User Configurable Timeout On No Answer for Call Forwarding, page 4-10
- Setting Up and Placing a Call Without Using a SIP Proxy, page 4-11

Advanced Audio Configuration

The UDPTOS (specifies the default IP precedence of UDP packets) and AudioMode (audio operating mode) parameters allow you to tune audio configuration.

Related Parameters

UDPTOS, page 5-32

AudioMode, page 5-20

Billable Features

You can customize specific features on a subscription basis by changing the values of specific bits in several different parameters. Table 4-2 contains a list of billable features and their related parameters:

Table 4-2 Billable Features and Related Parameters

Feature	Related Parameters
Call Conferencing	PaidFeatures, page 5-24, CallFeatures, page 5-23
Call Forwarding	PaidFeatures, page 5-24, CallFeatures, page 5-23, ConnectMode, page 5-28, SigTimer, page 5-32
Call Transfer	PaidFeatures, page 5-24, CallFeatures, page 5-23
Call Waiting	PaidFeatures, page 5-24, CallFeatures, page 5-23, SigTimer, page 5-32
Caller ID	PaidFeatures, page 5-24, CallFeatures, page 5-23, CallerIdMethod, page 5-25
Call Return	ConnectMode, page 5-28, PaidFeatures, page 5-24, CallFeatures, page 5-23
Polarity	Polarity, page 5-27
Voice Mail Indicator	PaidFeatures, page 5-24, CallFeatures, page 5-23



Note

CallWaitCallerID is an obsolete parameter. Do not use it.

Comfort Noise During Silence Period When Using G.711

When silence suppression is turned on in ITU G.711, the Cisco ATA calculates and transmits its noise level to the far end to enable the remote endpoint to generate the appropriate amount of comfort noise. This provides the remote user with a similar experience to that of a PSTN call and prevents silent gaps when neither party is talking.

Related Parameter

AudioMode, page 5-20—Bit 0 disables/enables silence suppression.

Configurable Hook Flash Timing

This feature provides the ability to adjust the hook-flash timing to meet local requirements.

Related Parameter

SigTimer, page 5-32—Bits 26 and 27 are for configuring the minimum on-hook time required for a hook flash event, and bits 28 through 31 are for configuring maximum on-hook time.

Configurable Mixing of Call Waiting Tone and Audio

This feature allows the call-waiting tone to be mixed with the audio in an active call. Therefore, the call-waiting tone will sound without a pause in the audio.

Related Parameter

ConnectMode, page 5-28—Bit 24

Configurable On-hook delay

This feature is available only for the recipient (callee) of a call. If the callee picks up the phone and then later hangs up to retrieve another call, the hang-up is not considered on-hook until the specified delay expires.

Related Parameter

FeatureTimer, page 5-26—Bits 8 to 12

Debugging Diagnostics

You can use the following parameters to troubleshoot operation issues:

- NPrintf, page 5-36—Specify the IP address and port where debug information is sent.
- TraceFlags, page 5-36—Use to turn on specific trace features.

Dial Plan

You can set specific dial plan rules and timeout values. Many of these values are determined on a country-by-country basis.

Related Parameter

DialPlan, page 5-38

Disabling Access To The Web Interface

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

Related Parameter

OpFlags, page 5-34—Bit 7

Distinctive Ringing

This feature allows a user to identify a caller based on the ringing pattern the user selects for the incoming number.

This feature is dependent on the proxy or remote UA, including the Alert-Info header with the appropriate value in the INVITE message. The Cisco ATA supports standard distinctive ringing pattern 1 to 5 as defined in the standard *GR-506-CORE*.

The following Alert-Info header values are allowed:

- Bellcore-dr1
- Bellcore-dr2
- Bellcore-dr3
- Bellcore-dr4
- Bellcore-dr5

If the Alert-Info header value is not recognized, the Cisco ATA plays the regular ring tone, Bellcore-dr1.

**Note**

The Bellcore-dr5 ringing pattern is the same as the Bellcore-dr1 ringing pattern.

DNS SRV Support

The Cisco ATA supports DNS SRV lookup for the SIP proxy server. If the GkOrProxy parameter value begins with _sip._udp. or sip.udp., the Cisco ATA performs a DNS SRV lookup for the SIP proxy server. A DNS SRV lookup results in one of the following conditions:

- Zero host is returned or DNS SRV lookup failed. The Cisco ATA then performs a regular DNS A-record lookup for the given name.
- One host is returned. The single host is used as the primary proxy and AltGk is the backup proxy, if specified.

- Two or more hosts are returned. The two hosts with the highest priorities are used as the primary and backup proxy servers (AltGk is ignored in this case).

Related Parameters

- GkOrProxy, page 5-10
- AltGk, page 5-13

Hardware Information Display

Cisco ATA hardware information is displayed in the lower-left corner of the Cisco ATA Web configuration page.

NAT Gateway

Network Address Translation (NAT) supports port mapping and forwarding to standard default SIP signaling port 5060 and media base port 16384, or other ports as configured in the Cisco ATA. Media ports are evenly numbered from the base port. NAT must support multiple port mappings. The Cisco ATA can use up to four media ports to handle conference calls on both lines. For example, if media base port 16384 is used for one call, the next call uses port 16386 and other calls will use ports 16388 and 16390.

**Note**

Routers such as D-Link, WinRoute, and WinProxy may not route correctly if both caller and callee are behind the same NAT.

To configure the Cisco ATA to work in a NAT environment, modify the following parameters:

- StaticRoute, page 5-7—Enter the LAN IP address of the NAT through which the Cisco ATA will communicate.
- NATIP, page 5-16—Enter the WAN IP address of the NAT through which all external SIP user agents will communicate.
- SIPPort, page 5-17—Enter a new port for SIP messages (optional).
- MediaPort, page 5-17—Enter a new base port for RTP media (optional).

NAT/PAT Translation

To maintain Network Address Translation/Port Address Translation (NAT/PAT) for a session, the Cisco ATA can be configured to periodically send a dummy UDP packet to a server (the Cisco ATA does not expect any response from the server).

Related Parameters

- NatTimer, page 5-19—Bits 0 to 11 are for specifying the retransmission period.
- NatServer, page 5-18—Specify the server to which the dummy packet is sent.

Network Timing

You can fine tune your network timing with the following parameters:

- **TimeZone**, page 5-30—Use for time-stamping incoming calls (offset from Greenwich Mean Time) with local time.
- **NTPIP**, page 5-30—Use for configuring the IP address of the Network Time Protocol server. NTP is a protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet.
- **AltNTPIP**, page 5-31—Use to configure an alternate NTP server IP address.
- **ConnectMode**, page 5-28—Used to control the connection mode of the SIP protocol.

OutBoundProxy Support

If the **OutBoundProxy** parameter is a fully qualified domain name (FQDN), and DNS returns multiple IP addresses, the first IP address is used as the primary outbound proxy and the second IP address as the secondary outbound proxy. If **OutBoundProxy** is an IP address or if DNS returns only one IP address, then a backup outbound proxy is not available. The **AltGkTimeOut** parameter determines the backup proxy timeout value for the outbound proxy.

If the backup proxy fails, the Cisco ATA automatically switches back to the primary proxy if the unit has been using the backup proxy for at least 30 seconds. This effectively prevents the Cisco ATA from switching indefinitely between failing primary and failing backup proxies for the same transactions.

Switching between primary and secondary proxies can occur only for initial INVITE and REGISTER requests. Other requests, such as CANCEL, BYE, ACK, and re-INVITE, do not retry the backup proxy but give up if the current proxy fails.

When **OutBoundProxy** is enabled, the Cisco ATA determines whether to retry to connect with the backup **OutBoundProxy** or backup SIP proxy if the INVITE or REGISTER requests fail. If the reason for failure is an ICMP error (such as an unreachable host), the Cisco ATA retries with the backup outbound proxy. If failure is due to timeout while waiting for a response or a 5xx response, the Cisco ATA retries the backup SIP proxy.

Related Parameter

- **OutBoundProxy**, page 5-17
- **AltGkTimeOut**, page 5-13

Progress Tones

Values for the following parameters (all defined in the “Call-Progress Tone Parameters” section on page 5-42) must be determined based on the country in which the Cisco ATA is located:

- **DialTone**
- **BusyTone**
- **ReorderTone**
- **RingBackTone**
- **CallWaitTone**
- **AlertTone**

Receiver-tagged VIA header

You can disable or enable the processing the *received* = parameter in the Via header. This feature is disabled by default.

Related Parameter

ConnectMode, page 5-28—Bit 22

Repeat Dialing on Busy Signal

This feature allows the Cisco ATA to repeatedly call a busy number at a periodic interval for a specific length of time. Both the interval and total time can be specified by the user.

To use this feature, configure FeatureTimer bits 0-7 and add the new command/action values "#37#;kA" to the existing "H" context and "5;jA" to the existing "S" context in the CallCmd parameter.

This feature is invoked by pressing 5 after the busy tone sounds. The caller then gets a beep confirmation followed by silence. When the subscriber hangs up, the Cisco ATA starts to redial at the interval specified in FeatureTimer bits 4-7. When the called party rings, the caller is notified with a special ring. If the called party picks up the call first, the called party receives a ringback. If the caller picks up the call first, the caller receives the ringback. This feature is automatically cancelled when the called party rings.



Note

For this feature to work properly, the remote user agent server must return a **486** (Busy Here) response to an INVITE request if it detects that the remote party (IP or PSTN) is busy. If the server returns a **183** (Session Progress) response with an SDP before a **486**, the Cisco ATA considers the call successful and automatically cancels repeat dialing.

Related Parameters

- FeatureTimer, page 5-26—Bits 0 to 3 control the maximum time the Cisco ATA redials a number.
- FeatureTimer, page 5-26—Bits 4 to 7 control the interval between each redial that the Cisco ATA performs. A value of zero (0) sets the default redial interval to 15 seconds.
- CallCmd, page 5-47—The following context commands are used as follows:

```
Parameter:      CallCmd
Context:        S (may also include 'a' or 'b')
Command/action: 5;jA
Description:    This context command adds the service activation code to enable
repeat dialing.

Parameter:      CallCmd
Context:        H
Command/action: #37#;kA
Description:    This context command adds the service deactivation code to disable
repeat dialing
```



Note

For complete information about call commands, see Chapter 6, "Call Commands."

SIP Proxy Server Redundancy

SIP proxy server redundancy can be enabled by entering a fully qualified domain name (FQDN) or IP address (and optional port number) in the GkOrProxy and AltGk parameters, and by configuring the AltGkTimeOut parameter. If you provide hostnames for GkOrProxy or AltGk, the names are resolved by the configured DNS. DNS results are hard-coded in cache memory for 10 minutes.

If DNS returns multiple IP addresses, the Cisco ATA uses only the first IP address. If AltGk is set to 0 (disabled) and DNS returns two or more IP addresses for GkOrProxy, then the Cisco ATA uses the first IP address as the primary proxy and the second IP address as the secondary proxy. If GkOrProxy is an IP address or DNS returns one IP address, then the backup SIP proxy is not available. A special case exists if GkOrProxy and AltGk are the same values and are not IP addresses. In this case, the AltGk parameter is assumed to have the value 0.

Related parameters

- GkOrProxy, page 5-10
- AltGk, page 5-13
- AltGkTimeOut, page 5-13

Stuttering Dial Tone on Unconditional Call Forward

If unconditional call forwarding is enabled, the Cisco ATA plays a continuous stuttering dial tone when the telephone handset is picked up. This reminds the user that all incoming calls are forwarded to another number. For more information, see the “Call Forwarding in the United States” section on page A-5 and the “Call Forwarding in Sweden” section on page A-6.

User Configurable Call Waiting Permanent Default Setting

This feature allows you to specify the default call-waiting setting for every call on a permanent basis by means of the service activation and deactivation codes.

Related Parameter

ConnectMode, page 5-28—Bit 23

User Configurable Timeout On No Answer for Call Forwarding

This feature allows you to specify the timeout before a call is forwarded to another number on no answer.

This feature is activated by entering the service activation code followed by the phone number and delay. The entry sequence is as follows:

```
<Service Activation Code> <Phone Number> * <Delay> #
```

Delay can be from 1 to 255 seconds. If the delay is zero (0) or not provided by the user, the delay specified in the SigTimer parameter (bits 20-25), which has a default value of 20 seconds, is in effect.

Example

Using the U.S. Call Command parameter string, the U.S. service activation code is #75 and the deactivation code is #73.

To forward calls to the number 555-1212 after a no-answer for 15 seconds, enter the following:

```
#755551212*15#
```

To deactivate this feature, enter the following:

```
#73
```

Related Parameter

SigTimer, page 5-32—Bits 20 to 25

Setting Up and Placing a Call Without Using a SIP Proxy

The Cisco ATA supports direct IP-to-IP calls without using a SIP proxy. When a call is placed, the Cisco ATA sends the INVITE request directly to the remote user agent and expects the usual 100/180/200 responses from the user agent.

This section contains the following topics:

- Configuration, page 4-11
- Placing an IP Call, page 4-12

Configuration

To perform the necessary configuration of the Cisco ATA, follow this procedure:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Open your Web browser. |
| Step 2 | Enter the URL: <code>http://<Cisco_ATA_IP_address>/dev</code>
where <code>Cisco_ATA_IP_address</code> is the IP address of your Cisco ATA. This takes you to the Cisco ATA Web configuration page. |
| Step 3 | Configure the following parameters as shown: <ul style="list-style-type: none">• GkOrProxy, page 5-10—Set to the value of 0 (zero).• UID0, page 5-9—Set to the unique telephone number of the Phone 1 port of the Cisco ATA.• UID1, page 5-9—Set to the unique telephone number of the Phone 2 port of the Cisco ATA.• UseSIP, page 5-14—Set to 1 to enable SIP mode.• SIPRegOn, page 5-16—Set to 0 to disable SIP registration with a SIP proxy server. |
| Step 4 | Click the Apply button to save these changes. |
-

Placing an IP Call

To place an IP call, dial the telephone number and the IP address of the remote user agent. The dial format is shown below:

Dial Format

`<phone number>**<ipaddress>#`

Use the star (*) key on the telephone keypad to represent the dot (.) in an IP address. Use the pound (#) key on the telephone keypad to terminate the dial string and place the call.



Note

URL dialing is not supported.

Example

To place a call to a user agent with an ID of 408-555-1212 at IP address 192.168.1.100, you would enter the following string on your telephone keypad:

4085551212192*168*1*100#**

Complete Reference Table of all Cisco ATA SIP Services

Table 4-3 is a reference table that lists all configurable features for the Cisco ATA (using SIP), and includes links to the detailed descriptions of the parameters used for configuring these features.

Table 4-3 Configurable Features and Related Parameters

Configurable Feature	Related Parameter
802.1Q packet tagging	VLANSetting, page 5-35
Audio compression and decompression	LBRCCodec, page 5-20
Backup proxy configuration	AltGk, page 5-13
Backup proxy timeout	AltGkTimeOut, page 5-13
Call forward enable/disable	ConnectMode, page 5-28
Call forwarding—Maximum times allowed	MAXRedirect, page 5-15
Call commands	CallCmd, page 5-47, Chapter 6, “Call Commands”
Call features	CallFeatures, page 5-23
Caller ID format	CallerIdMethod, page 5-25
Call waiting	SigTimer, page 5-32
Call-waiting call ring timeout	FeatureTimer, page 5-26
Call-waiting state specified	ConnectMode, page 5-28
Cisco Discovery Protocol	OpFlags, page 5-34
CNG tone detection	AudioMode, page 5-20
Configuration update interval	CfgInterval, page 5-5
Debug messages—configuring host	NPrintf, page 5-36

Table 4-3 Configurable Features and Related Parameters (continued)

Configurable Feature	Related Parameter
Dial plan commands	DialPlan, page 5-38
Domain name server	DNS1IP, page 5-31
DNS hostname lookup	ConnectMode, page 5-28
DTMF method	AudioMode, page 5-20
Encryption	EncryptKey, page 5-6
Fax CED tone	AudioMode, page 5-20
Fax mode on a per-call basis	CallFeatures, page 5-23, PaidFeatures, page 5-24
Fax pass-through	AudioMode, page 5-20, ConnectMode, page 5-28
G.711 codec	AudioMode, page 5-20
Hook flash	AudioMode, page 5-20, SigTimer, page 5-32
IDs for phone lines	UID0, page 5-9, UID1, page 5-9
IP-like address in dial plan	IPDialPlan, page 5-38
Login ID	LoginID0, page 5-12, LoginID1, page 5-12
Low bit-rate codec	LBRCCodec, page 5-20
Mixing of tones	ConnectMode, page 5-28
Network Address Translation (NAT) server—Maintain during session	NatServer, page 5-18
NSE payload number	ConnectMode, page 5-28
NTP IP address	NATIP, page 5-16
On-hook delay	FeatureTimer, page 5-26
Outbound proxy	OutBoundProxy, page 5-17
Paid features	PaidFeatures, page 5-24
Passwords for phone lines	PWD0, page 5-9, PWD1, page 5-10
Polarity	Polarity, page 5-27
Polarity reversal before and after caller ID signal	CallerIdMethod, page 5-25
<i>Received</i> = tag enable/disable	ConnectMode, page 5-28
Receiving-audio codec preference	RxCodec, page 5-21
Redial time if line is busy	FeatureTimer, page 5-26
Refresh Cisco ATA using Web server	OpFlags, page 5-34
REGISTER messages	ConnectMode, page 5-28
Registration removal	ConnectMode, page 5-28
Reset Cisco ATA using Web server	OpFlags, page 5-34
Retransmission interval for NAT server	NatTimer, page 5-19

Table 4-3 Configurable Features and Related Parameters (continued)

Configurable Feature	Related Parameter
Dial plan commands	DialPlan, page 5-38
Domain name server	DNS1IP, page 5-31
DNS hostname lookup	ConnectMode, page 5-28
DTMF method	AudioMode, page 5-20
Encryption	EncryptKey, page 5-6
Fax CED tone	AudioMode, page 5-20
Fax mode on a per-call basis	CallFeatures, page 5-23, PaidFeatures, page 5-24
Fax pass-through	AudioMode, page 5-20, ConnectMode, page 5-28
G.711 codec	AudioMode, page 5-20
Hook flash	AudioMode, page 5-20, SigTimer, page 5-32
IDs for phone lines	UID0, page 5-9, UID1, page 5-9
IP-like address in dial plan	IPDialPlan, page 5-38
Login ID	LoginID0, page 5-12, LoginID1, page 5-12
Low bit-rate codec	LBRCCodec, page 5-20
Mixing of tones	ConnectMode, page 5-28
Network Address Translation (NAT) server—Maintain during session	NatServer, page 5-18
NSE payload number	ConnectMode, page 5-28
NTP IP address	NATIP, page 5-16
On-hook delay	FeatureTimer, page 5-26
Outbound proxy	OutBoundProxy, page 5-17
Paid features	PaidFeatures, page 5-24
Passwords for phone lines	PWD0, page 5-9, PWD1, page 5-10
Polarity	Polarity, page 5-27
Polarity reversal before and after caller ID signal	CallerIdMethod, page 5-25
<i>Received</i> = tag enable/disable	ConnectMode, page 5-28
Receiving-audio codec preference	RxCodec, page 5-21
Redial time if line is busy	FeatureTimer, page 5-26
Refresh Cisco ATA using Web server	OpFlags, page 5-34
REGISTER messages	ConnectMode, page 5-28
Registration removal	ConnectMode, page 5-28
Reset Cisco ATA using Web server	OpFlags, page 5-34
Retransmission interval for NAT server	NatTimer, page 5-19

Table 4-3 Configurable Features and Related Parameters (continued)

Configurable Feature	Related Parameter
Retry interval if line is busy	FeatureTimer, page 5-26
Ringback tone—send to caller	ConnectMode, page 5-28
Ring-cadence pattern	RingOnOffTime, page 5-37
RTP media port	MediaPort, page 5-17
RTP packet size	NumTxFrames, page 5-22
RTP statistics	TraceFlags, page 5-36
Secondary domain name server	DNS2IP, page 5-31
Silence compression	AudioMode, page 5-20
SIP call return	ConnectMode, page 5-28
SIP mode	UseSIP, page 5-14
SIP proxy registrar address	GkOrProxy, page 5-10
SIP proxy registration renewal	SIPRegInterval, page 5-15
SIP registration enable/disable	SIPRegOn, page 5-16
SIP-request listening port	SIPPort, page 5-17
Static network router probe	OpFlags, page 5-34
TFTP file—not using internally generated name	OpFlags, page 5-34
Timeout values	SigTimer, page 5-32
Time zone offset	TimeZone, page 5-30
Tones: BusyTone, CallWaitTone AlertTone, DialTone, ReorderTone, and RingBackTone parameters	Call-Progress Tone Parameters, page 5-42
Tracing	TraceFlags, page 5-36
Transmitting-audio codec preference	TxCodec, page 5-22
UDP packet default IP precedence	UDPTOS, page 5-32
VLAN encapsulation	OpFlags, page 5-34
VLAN mode	OpFlags, page 5-34
WAN address of NAT	NATIP, page 5-16
Web configuration—disallowing	OpFlags, page 5-34



Parameters and Defaults

This section provides information on the parameters and defaults that you can use to create your own Cisco ATA configuration file. This section also includes the voice configuration menu code for each parameter that has such a code, and each category of parameter type lists the color portion of the web configuration screen where the parameter is located. Types of parameters include:

- User Interface (UI) Parameter, page 5-3
- Configuration Parameter, page 5-4
- Parameters for Configuration Method, page 5-4
- Network Parameters, page 5-6
- Account Information Parameters, page 5-8
- Backup Server Parameters, page 5-13
- SIP Parameters, page 5-14
- Operating Parameters, page 5-19
- Optional Feature Parameters, page 5-35

The following list contains general configuration information:

- Your configuration file must begin with **#txt**.
- The Cisco ATA uses the following parameter types:
 - Alphanumeric string
 - Array of short integers
 - Boolean (1 or 0)
 - Bitmap value—unsigned hexadecimal integer (for specifying bits in a 32-bit integer)
 - Extended IP address—IP address followed by port number (for example, 192.168.2.170.9001)
 - IP address (e.g. 192.168.2.170)
 - Integer (32-bit integer)
 - Numeric digit string



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.

**Note**

This section contains recommended values for the United States and Sweden as configuration examples for certain parameters. For information about other countries, contact the Cisco equipment provider for a specific country.

Configuration Text File Template

This is a listing of the example_uprofile.txt text file, without its annotations, that comes bundled with the Cisco ATA software.

You can make a copy of this file and use it as a template for creating your own default configuration file or Cisco ATA-specific configuration file. For instructions on how to create these configuration files, see the “Creating Unique and Common Cisco ATA Configuration Files” section on page 3-8.

The example_uprofile.txt file contains all the Cisco ATA default values. The sections that follow this listing describe all the parameters in this file.

```
#txt
UIPassword:0
UseTftp:1
TftpURL:0
cfgInterval:3600
EncryptKey:0
ToConfig:0
upgradecode:0,0x301,0x0400,0x0200,0.0.0.0,69,0,none
upgradelang:0,0x301,0x0400,0x0200,0.0.0.0,69,0,none
Dhcp:1
StaticIp:0
StaticRoute:0
StaticNetMask:0
GkOrProxy:0
AltGk:0
AltGkTimeOut:0
GkTimeToLive:300
GateWay:0
GateWay2:0.0.0.0
UseLoginID:0
UID0:0
UID1:0
PWD0:0
PWD1:0
LoginID0:0
LoginID1:0
GkId:.
RxCodec:1
TxCodec:1
LBRCodec:0
AudioMode:0x00150015
NumTxFrames:2
CallWaitCallerId:0x003c33d0
Polarity: 0
ConnectMode:0x00060000
AutMethod:0
TimeZone:17
NTPIP:0
AltNTPIP:0
DNS1IP:0.0.0.0
DNS2IP:0.0.0.0
UDPTOS:0xA0
```

```

RingOnOffTime:2,4,25
DialTone:2,31538,30831,1380,1740,1,0,0,1500
BusyTone:2,30467,28959,1191,1513,0,4000,4000,0
ReorderTone:2,30467,28959,1191,1513,0,2000,2000,0
RingBackTone:2,30831,30467,1943,2111,0,16000,32000,0
CallWaitTone:1,30831,0,5493,0,0,2400,2400,4800
AlertTone:1,30467,0,5970,0,0,480,480,1920
DialPlan:*St4-|#St4-|911|1>#t8.r9t2-|0>#t811.rat4-|^1t4>#.-
IPDialPlan: 1
CallCmd:Af;AH;BS;NA;CS;NA;Df;EB;Ff;EP;Kf;EFh;HQ;Jf;AFh;HQ;I*67;gA*82;fA#90v#;OI;H#72v#;bA#
74v#;cA#75v#;dA#73;eA*67;gA*82;fA*70;iA*69;DA*99;xA;Uh;GQ;
SIPPort:5060
SIPRegOn:0
SIPRegInterval:120
MaxRedirect:5
OutBoundProxy:0
NatServer:0
NatTimer:0
NPrintf:0
TraceFlags:0x00000000
EchoIP:192.168.2.9
SigTimer:0x01418564
OpFlags:0x2
VLANSetting:0x0000002b
FeatureTimer:0x00000000

```

The sections that follow describe these parameters.

User Interface (UI) Parameter

This parameter is located in the purple portion of the Cisco ATA Web Configuration Page.

UIPassword

Description

This parameter controls access to web page or voice configuration menu interface. To set a password, enter a value other than zero. To have the user prompted for this password when attempting to perform a factory reset or upgrade using the voice configuration menu, see the “OpFlags” section on page 5-34.

To clear a password, change the value to 0.

You cannot recover a forgotten password unless you reset the entire configuration of the Cisco ATA (see the “Resetting the Cisco ATA to Factory Default Values” section on page 3-18). If you forget a password, you can contact your Cisco representative.



Note

When UIPassword contains letters, you cannot enter the password from the telephone keypad.

Value Type

Alphanumeric string

Range

Maximum nine characters

Default

0

Voice Configuration Menu Access Code

7387277

Configuration Parameter

This parameter is located in the light-yellow portion of the Cisco ATA Web Configuration Page.

ToConfig

Description

After you configure the Cisco ATA, set the parameter to 0, or the Cisco ATA will unnecessarily contact the TFTP server.

Value Type

Boolean

Range

0 or 1

Default

1—This indicates that the operating parameters have not previously been set.

Voice Configuration Menu Access Code

80001

Parameters for Configuration Method

This section describes the following parameters, which are located in the grey portion of the Cisco ATA Web Configuration Page:

- UseTFTP, page 5-4
- TftpURL, page 5-5
- CfgInterval, page 5-5
- EncryptKey, page 5-6

UseTFTP

Settings

1—Use the TFTP server for Cisco ATA configuration.

0—Do not use the TFTP server for Cisco ATA configuration.

Value Type

Boolean

Range

0 or 1

Default

1

Voice Configuration Menu Access Code

305

TftpURL

Description

Use this parameter to specify the IP address or URL of the TFTP server. This string is needed if the DHCP server does not provide the TFTP server IP address. When the TftpURL parameter is set to a non-zero value, this parameter has priority over the TFTP server IP address supplied by the DHCP server.

Optionally, you can include the path prefix to the TFTP file to download.

For example, if the TFTP server IP address is 192.168.2.170 or www.cisco.com, and the path to download the TFTP file is in /ata186, you can specify the URL as 192.168.2.170/ata186 or www.cisco.com/ata186.

**Note**

From the voice configuration menu, you can only enter the IP address; from the web server, you can enter the actual URL.

Value Type

Alphanumeric string

Range

Maximum number of characters: 31

Default

0

Voice Configuration Menu Access Code

905

CfgInterval

Description

Use this parameter to specify the number of seconds between each configuration update. The Cisco ATA will also upgrade its signaling image if it detects that the TFTP server contains an upgraded image.

For example, when using TFTP for configuration, the Cisco ATA contacts TFTP each time the interval expires to get its configuration file.

You can set CfgInterval to a random value to achieve random contact intervals from the Cisco ATA to the TFTP server.

Value Type

Decimal

Range

60 to 4294967295

Default

3600

Voice Configuration Menu Access Code

80002

EncryptKey

Description

This parameter specifies the encryption key that is used to encrypt the Cisco ATA configuration file on the TFTP server.

The cfgfmt tool, which is used to create a Cisco ATA binary configuration file (see the “Using the EncryptKey Parameter and cfgfmt Tool” section on page 3-11), automatically encrypts the binary file, using the rc4 encryption algorithm, when the EncryptKey parameter has a value other than 0.

**Note**

If the Cisco ATA configuration file is not encrypted, the value must be set to 0.

Value Type

Alphanumeric string

Range

Maximum number of characters: 8

Default

0

Voice Configuration Menu Access Code

320

Network Parameters

This section describes the following parameters, which are located in the orange portion of the Cisco ATA Web Configuration Page:

- DHCP, page 5-7
- StaticIp, page 5-7

- StaticRoute, page 5-7
- StaticNetMask, page 5-8

DHCP

Description

A DHCP server can be used to automatically set the Cisco ATA IP address, the network route IP address, the subnet mask, DNS, NTP, TFTP, and other parameters.

- 1—Enable DHCP
- 0—Disable DHCP

Value Type

Boolean

Range

0 or 1

Default

1

Voice Configuration Menu Access Code

20

StaticIp

Description

Use this parameter to statically assign the Cisco ATA IP address if the DHCP parameter is set to 0.

Value Type

IP address

Default

0.0.0.0

Voice Configuration Menu Access Code

1

StaticRoute

Description

Use this parameter to statically assign the Cisco ATA route if the DHCP parameter is set to 0.

Value Type

IP address

Default

0.0.0.0

Voice Configuration Menu Access Code

2

StaticNetMask

Description

Use this parameter to statically assign the Cisco ATA subnet mask if the DHCP parameter is set to 0

Value Type

IP address

Default

255.255.255.0

Voice Configuration Menu Access Code

10

Account Information Parameters

This section describes the following parameters, which are located in the blue portion of the Cisco ATA Web Configuration Page:

- UID0, page 5-9
- PWD0, page 5-9
- UID1, page 5-9
- PWD1, page 5-10
- GkOrProxy, page 5-10
- Gateway, page 5-11
- Gateway2, page 5-11
- UseLoginID, page 5-11
- LoginID0, page 5-12
- LoginID1, page 5-12

UID0

Description

This parameter is the User ID for the **Phone 1** port. If the value is set to zero, the port will be disabled and no dial tone will sound.

Value Type

Alphanumeric string

Range

Maximum number of characters: 31

Default

0

Voice Configuration Menu Access Code

3

PWD0

Description

This parameter is the password for the **Phone 1** port.

Value Type

Alphanumeric string

Range

Maximum number of characters: 31

Default

0

Voice Configuration Menu Access Code

4

UID1

Description

This parameter is the User ID for the **Phone 2** port. If the value is set to zero, the port will be disabled and no dial tone will sound.

Value Type

Alphanumeric string

Range

Maximum number of characters: 31

Default

0

Voice Configuration Menu Access Code

13

PWD1

Description

This parameter is the password for the **Phone 2** port.

Value Type

Alphanumeric string

Range

Maximum number of characters: 31

Default

0

Voice Configuration Menu Access Code

14

GkOrProxy

Description

This parameter is the proxy address or registrar address.

For a SIP proxy server, this can be an IP address with or without a port parameter such as 123.123.110.45, 123.123.110.45.5060, or 123.123.110.45:5061, or a URL such as sip.cisco.com, or sip.ata.cisco.com:5061. For an IP address, a '.' or ':' can be used to delimit a port parameter. For a URL, a ':' must be used to indicate a port.

**Note**

If the SIP proxy server and registration server reside on separate hardware, enter the SIP registration server address in this field.

If the hostname specified in GkOrProxy has a prefix of _sip._udp or sip.udp, the Cisco ATA first attempts to perform a DNS SRV lookup on the hostname.

If the SRV lookup returns two hosts, they become primary and backup proxies according to their priority (as specified in the DNS SRV RFC), and the hostname specified in the AltGk parameter is ignored.

If the SRV lookup returns only one host, this host is the primary proxy, and the hostname specified in the AltGk parameter is the backup proxy.

Value Type

Alphanumeric string

Range

Maximum number of characters: 31

Default

0—Disables proxy registration and proxy-routed calls.

In this case, you can make direct IP calls by dialing the user-id@IP:port of the callee, where user-id must be a numeric value, '@' is dialed as "**", and '.' and ':' are dialed as a '*'.

The following list shows some examples of direct SIP IP dialing:

- 1234**192*168*1*10*5060
- 102*210*9*101*5061
- 4084281002**100*123*89*10

Voice Configuration Menu Access Code

5

Gateway

Description

Not applicable to SIP.

Gateway2

Description

Not applicable to SIP.

UseLoginID

Description

0—Use UID0 and UID1 as the authentication ID.

1—Use LoginID0 and LoginID1 as the authentication ID.

Value Type

Boolean

Range

0 or 1

Default

0

Voice Configuration Menu Access Code

93

LoginID0

Description

This parameter is the Login ID for line 0.

**Note**

UID0 is used for authentication if UseLoginID is 0.

Value Type

Alphanumeric string

Range

Maximum number of characters: 51

Default

0

Voice Configuration Menu Access Code

46

LoginID1

Description

This parameter is the Login ID for line 1.

**Note**

UID1 is used for authentication if UseLoginID is 0.

Value Type

Alphanumeric string

Range

Maximum number of characters: 51

Default

0

Voice Configuration Menu Access Code

47

Backup Server Parameters

This section describes the following parameters, which are located in the lavender portion of the Cisco ATA Web Configuration Page:

- AltGk, page 5-13
- AltGkTimeOut, page 5-13
- GkTimeToLive, page 5-14
- GkId, page 5-14

AltGk

Description

You have the option of using this parameter to specify a backup proxy. However, if a DNS SRV performed on the GkOrProxy parameter returns more than one host, the AltGk parameter is ignored.

Value Type

Alphanumeric string

Range

Maximum number of characters: 31

Default

0

Voice Configuration Menu Access Code

6

AltGkTimeOut

Description

You can use this parameter to specify the timeout in seconds before the Cisco ATA fails back to the primary proxy server from the backup proxy server. Re-registration does not occur until the current registration period expires.

Value Type

Integer

Default

0—The Cisco ATA continues to use the backup proxy server until it fails before attempting to fail back to the primary proxy server.

Range

30 to 4294967295 seconds

Voice Configuration Menu Access Code

251

GkTimeToLive

Description

Not applicable to SIP.

GkId

Description

Not applicable to SIP.

SIP Parameters

This section describes the following parameters, which are located in the yellow portion of the Cisco ATA Web Configuration Page:

- UseSIP, page 5-14
- SIPRegInterval, page 5-15
- MAXRedirect, page 5-15
- SIPRegOn, page 5-16
- NATIP, page 5-16
- SIPPort, page 5-17
- MediaPort, page 5-17
- OutBoundProxy, page 5-17
- NatServer, page 5-18
- NatTimer, page 5-19

UseSIP

Description

0—Use H.323 mode.

1—Use SIP mode.

Value Type

Boolean

Range

0 or 1

Default

0

Voice Configuration Menu Access Code

38

SIPRegInterval

Description

Use this parameter to configure the number of seconds between Cisco ATA registration renewal with the SIP proxy server. The Cisco ATA renews the registration at some percentage of time earlier than the specified interval to prevent a registration from expiring.

Value Type

Integer

Range

1 to 86400

Default

3600

Voice Configuration Menu Access Code

203

MAXRedirect

Description

This parameter specifies the maximum number of times that a called number is allowed to forward the call to another number.

Value Type

Integer

Range

0 to 10

Default

5

Voice Configuration Menu Access Code

205

SIPRegOn

Description

0—Disable SIP registration.

1—Enable SIP registration. When this flag is enabled, the Cisco ATA registers with the SIP Proxy Server that is specified in the GkorProxy parameter. The Cisco ATA also registers with the interval that is specified in the SIPRegInterval parameter.

Value Type

Boolean

Range

0 or 1

Default

0

Voice Configuration Menu Access Code

204

NATIP

Description

This is the WAN address of the attached router/NAT; currently only used to support SIP behind a NAT.

Value Type

IP address

Default

0.0.0.0

Voice Configuration Menu Access Code

200

SIPPort

Description

This parameter is used to configure the port through which the Cisco ATA listens for incoming SIP requests and sends outgoing SIP requests.

Value Type

Integer

Range

1 to 65535

Default

5060

Voice Configuration Menu Access Code

201

MediaPort

Description

Use this parameter to specify the base port where the Cisco ATA transmits and receives RTP media. This parameter *must* be an even number. Each connection uses the next available even-numbered port for RTP.

Value Type

Integer

Range

1 to 65535

Default

16384

Voice Configuration Menu Access Code

202

OutBoundProxy

Description

The SIP Outbound Proxy Server is a SIP proxy server which can be different from the Registration Proxy Server (specified in the GkOrProxy parameter) and to which all outgoing SIP requests are sent. Outgoing SIP responses are not affected by this out-bound-proxy and are still sent according to the VIA header and source address of the incoming SIP requests.

If the outgoing SIP request has a ROUTE header, the first route in the header is removed if it resolves to the same IP address as the out-bound-proxy. This process guards against the case when the out-bound-proxy also inserts its IP address into the RECORD-ROUTE header.

The OutBoundProxy parameter can be an IP address with or without a port parameter, such as 123.123.110.45, 123.123.110.45.5060, or 123.123.110.45:5061, or a URL such as sip.cisco.com, sip.ata.cisco.com:5061. For IP addresses, a period (.) or colon (:) can be used to delimit a port parameter. For a URL, a colon (:) must be used to indicate a port. If no port parameter is specified, the port 5060 is assumed.

Value Type

Alphanumeric string

Range

Maximum number of characters: 31

Default

0

Voice Configuration Menu Access Code

206

NatServer

Description

This parameter allows you to specify a server to which a dummy, single-byte UDP packet is sent to maintain a Network Address Translation (NAT) during a session.

NatServer can contain up to 47 characters in fully qualified domain name (FQDN) or IP format with an optional port parameter (separated from the address by a colon); for example, xyz.cisco.com:1234. If no port is specified, the default port of 5060 is assumed.

Value Type

IP address or FQDN format

Range

Maximum number of characters: 47

Default

5060 is the default port if no port is specified.

Voice Configuration Menu Access Code

207

NatTimer

Description

This parameter allows you to specify a retransmission interval for sending a dummy packet to NatServer. The interval is in seconds and is specified in bits 0-11 of this parameter. The upper 20 bits are reserved and should be set to 0.

Value Type

Bitmap

Default

0, which means that no dummy packets will be sent to the NatServer.

Voice Configuration Menu Access Code

208

Operating Parameters

This section describes the following parameters, which are located in the green portion of the Cisco ATA Web Configuration Page:

- LBRCodec, page 5-20
- AudioMode, page 5-20
- RxCodec, page 5-21
- TxCodec, page 5-22
- NumTxFrames, page 5-22
- CallFeatures, page 5-23
- PaidFeatures, page 5-24
- CallerIdMethod, page 5-25
- FeatureTimer, page 5-26
- Polarity, page 5-27
- ConnectMode, page 5-28
- AutMethod, page 5-30
- TimeZone, page 5-30
- NTPIP, page 5-30
- AltNTPIP, page 5-31
- DNS1IP, page 5-31
- DNS2IP, page 5-31
- UDPTOS, page 5-32
- SigTimer, page 5-32
- OpFlags, page 5-34
- VLANSetting, page 5-35

LBRCodec

Description

This parameter allows you to specify which low-bit-rate codecs are available. The Cisco ATA is capable of supporting two G.723.1 connections or one G.729 connection. When G.723.1 is selected as the low-bit-rate codec, each FXS port is allocated with one G.723.1 connection. When G.729 is selected, only one FXS port is capable of operating with the G.729 codec. The allocation of the G.729 resource to the FXS port is dynamic. The G.729 resource, if available, is allocated to an FXS port when a call is initiated or received; the resource is released when a call is completed.

The following values are valid:

- 0—Select G.723.1 as the low-bit-rate codec.
- 3—Select either G.729 as the low-bit-rate codec.

Related Parameters

- RxCCodec, page 5-21
- TxCodec, page 5-22

Value Type

Integer

Range

0 or 3

Default

0

Voice Configuration Menu Access Code

300

AudioMode

Description

This parameter represents the audio operating mode. The lower 16 bits are for the **Phone 1** port, and the upper 16 bits are for the **Phone 2** port. Table 5-1 on page 5-21 provides definitions for each bit.

Value Type

Bitmap

Default

0x00150015

Voice Configuration Menu Access Code

312

Table 5-1 AudioMode Parameter Bit Definitions

Bit Number	Definition
0	0/1—Disable/enable G.711 silence suppression.
1	0—Enable selected low-bit-rate codec in addition to G.711. This setting is the default. 1—Enable G.711 only.
2	0/1—Disable/enable fax CED tone detection.
3	0/1—Enable/disable fax CNG tone detection.
4-5: DtmfMethod	0—Always in-band (send and receive, do not send SDP info) 1—By negotiation (send SDP info, enable receive, decode others' SDP information, send depends on others' SDP information) 2—Always out-of-band (send SDP info, enable receive, decode others' SDP information, always send). 3—Reserved.
6-15	Reserved.

RxCodec

Description

Use this parameter to specify receiving-audio codec preference. The following values are valid:

- 0—G.723 (can be selected only if LBRCodec is set to 0)
- 1—G.711A-law
- 2—G.711 μ -law
- 3—G.729a (can be selected only if LBRCodec is set to 3)

Value Type

Integer

Range

0-3

Default

2

Voice Configuration Menu Access Code

36

TxCodec

Description

Use this parameter to specify the transmitting-audio codec preference. The following values are valid:

- 0—G.723 (can be selected only if LBRCodec is set to 0)
- 1—G.711A-law
- 2—G.711 μ -law
- 3—G.729A (can be selected only if LBRCodec is set to 3)

Value Type

Integer

Range

0-3

Default

2

Voice Configuration Menu Access Code

37

NumTxFrames

Description

Use this parameter to select the default RTP packet size in number of frames per packet. The Cisco ATA default frame sizes are as follows:

- G.711 and G.729—10 ms
- G.723.1—30 ms

For example, to receive 20 ms of G.729 packets, set the parameter to 2.

Value Type

Integer

Range

1-6

Default

2

Voice Configuration Menu Access Code

35

CallFeatures

Description

Disable/enable CallFeatures by setting each corresponding bit to 0 or 1.

The lower 16 bits are for the **Phone 1** port, and the upper 16 bits are for the **Phone 2** port. Table 5-2 provides definitions of each bit.



Note

The subscribed features that can be permanently disabled by the user are CLIP_CLIR, call waiting and Fax mode. A subscribed service enable/disabled by the user can be disabled/enabled dynamically on a per-call basis.

Value Type

Bitmap

Default

0xffffffff

Voice Configuration Menu Access Code

314

Table 5-2 CallFeatures Parameter Bit Definitions

Bit Number	Definition
0	Forward unconditionally
1	Forward on busy
2	Forward on no answer
3	CLIP_CLIR
4	Call waiting
5	three-way calling
6	Blind transfer
7	Transfer with consultation. This service allows the user to transfer the remote party to a different number by first calling that number and consulting with the callee.
8	Caller ID. This service enables the Cisco ATA 186 to generate a Caller ID signal to drive a Caller ID display device attached to the FXS line.
9	Call return
10	Message waiting indication
11	Call Waiting Caller ID. This is available only if the Method bit in CallerIdMethod is set to Bellcore (FSK).
15	Fax mode. This service allows the user to set the Cisco ATA to Fax mode on a per-call basis. For Fax mode, use the following settings: <ul style="list-style-type: none"> • G711 codec only • No silence suppression • No FAX tone detection

PaidFeatures

Description

Unsubscribe/subscribe to CallFeatures by setting each corresponding bit to either 0 or 1. The lower 16 bits are for the **Phone 1** port, and the upper 16 bits are for the **Phone 2** port. Table 5-3 provides definitions of each bit.

Value Type

Bitmap

Default

0xffffffff

Voice Configuration Menu Access Code

315

Table 5-3 PaidFeatures Parameter Bit Definitions

Bit Number	Definition
0	Forward unconditionally
1	Forward on busy
2	Forward on no answer
3	CLIP_CLIR
4	Call waiting
5	three-way calling
6	Blind transfer
7	Transfer with consultation. This service allows the user to transfer the remote party to a different number by first calling that number and consulting with the callee.
8	Caller ID. This service enables the Cisco ATA 186 to generate a Caller ID signal to drive a Caller ID display device attached to the FXS line.
9	Call return
10	Message waiting indication
11	Call Waiting Caller ID. This is available only if the Method bit in CallerIdMethod is set to Bellcore (FSK).
15	Fax mode. This service allows the user to set the Cisco ATA to Fax mode on a per-call basis. For Fax mode, use the following settings: <ul style="list-style-type: none"> • G.711 codec only • No silence suppression • No FAX tone detection

CallerIdMethod

Description

This 32-bit parameter specifies the signal format to use for both FXS ports for generating Caller ID format. Possible values are:

- Bits 0-1 (method)—0=Bellcore (FSK), 1=DTMF, values 2 and 3 are reserved.

If *method*=0, set the following bits:

- Bit 2—Reserved.
- Bit 3 to 8—Maximum number of digits in phone number (valid values are 1 to 20; default is 12)
- Bit 9 to 14—Maximum number of characters in name (valid values are 1 to 20; default is 15)
- Bit 15—If this bit is enabled (it is by default), send special character **O** (out of area) to CID device if the phone number is unknown.
- Bit 16—If this bit is enabled (it is by default), send special character **P** (private) to CID device if the phone number is restricted.
- Bits 17 to 27—Reserved.

If *method*=1, set the following bits:

- Bits 3-6—Start digit for known numbers (valid values are **12** for “A,” **13** for “B,” **14** for “C,” and **15** for “D.”)
- Bits 7-10—End digit for known numbers (valid values are **11** for “#,” **12** for “A,” **13** for “B,” **14** for “C,” and **15** for “D.”)
- Bits 11—Polarity reversal before and after Caller ID signal (value of 0/1 disables/enables polarity reversal)
- Bits 12-16—Maximum number of digits in phone number (valid values are 1 to 20)
- Bits 17 to 19—Start digit for unknown or restricted numbers (valid values are **4** for “A,” **5** for “B,” **6** for “C,” and **7** for “D.”)
- Bits 20 to 22—End digit for unknown or restricted numbers (valid values are **3** for “#,” **4** for “A,” **5** for “B,” **6** for “C,” and **7** for “D.”)
- Bits 23 to 24—Code to send to the CID device if the number is unknown (valid values are **0** for “00,” **1** for “0000000000,” and **2** for “2.” **3** is reserved and should not be used.
- Bits 25 to 26—Code to send to the CID device if the number is restricted (valid values are **0** for “10,” and **1** for “1.” **2** and **3** are reserved and should not be used.
- Bits 27 to 31—Reserved.

Examples

The following examples are recommended values for the CallerID Method parameter:

- USA=0x19e60
- Sweden=0x0ff61 or 0x006aff61
- Denmark=0x0fde1 or 0x033efde1

Value Type

Bitmap

Default

0x00019e60

Voice Configuration Menu Access Code

316

FeatureTimer

Description

This parameter provides configurable timing values for various features, as shown below.

- Bits 0-3—Maximum time to spend redialing if line is busy
 - Range: 0 - 15
 - Factor: five-minute increments
 - Values: 0 - 75 minutes
 - Default: 0 (= 30 minutes)
- Bits 4-7—Retry interval if line is busy
 - Range: 0 - 15
 - Factor: 15-second increments
 - Values: 0 - 225 seconds
 - Default: 0 (= 15 seconds)
- Bits 8-12—On-hook delay before a call is disconnected. This feature works only when the Cisco ATA is the terminating endpoint of the call. The user can hang up the phone in one room and pick up the phone in another room without disconnecting the line.
 - Range: 0 - 31
 - Factor: five-second increments
 - Values: 0 - 155 seconds
 - Default: 0 (no delay)
- Bits 13-15—Amount of time the Cisco ATA waits for a "486 Busy Here" response from a PSTN gateway after receiving a "183 Session Progress" response.
 - Range: 0 - 7
 - Factor: one-second increments
 - Values: 0 to 7 seconds
 - Default: 0 (no waiting)
- Bits 16-31—Reserved.

Value Type

Bitmap

Default

0x00000000

Voice Configuration Menu Access Code

317

Polarity

Description

You can control line polarity of the Cisco ATA FXS ports when a call is connected or disconnected by configuring the Polarity bitmap parameter as follows:

- Bit 0: CALLER_CONNECT_POLARITY. Polarity to use when the Cisco ATA is the caller and the call is connected.
 - 0 =Use forward polarity (Default)
 - 1 =Use reverse polarity
- Bit 1: CALLER_DISCONNECT_POLARITY. Polarity to use when the Cisco ATA is the caller and the call is disconnected.
 - 0 =Use forward polarity (Default)
 - 1 =Use reverse polarity
- Bit 2: CALLEE_CONNECT_POLARITY. Polarity to use when the Cisco ATA is the callee and the call is connected.
 - 0 =Use forward polarity (Default)
 - 1 =Use reverse polarity
- Bit 3: CALLEE_DISCONNECT_POLARITY. Polarity to use when the Cisco ATA is the callee and the call is disconnected.
 - 0 =Use forward polarity (Default)
 - 1 =Use reverse polarity

**Note**

Bits 4-31 are reserved.

Value Type

Bitmap

Default

0x00000000

Voice Configuration Menu Access Code

304

ConnectMode

Description

This parameter is a 32-bit bitmap used to control the connection mode of the selected call signaling protocol. Table 5-4 on page 5-28 provides bit definitions for this parameter.

Value Type

Bitmap

Default

0x00060400


Voice Configuration Menu Access Code

311

Table 5-4 ConnectMode Parameter Bit Definitions

Bit Number	Definition
0—H.323 only	0—Enable normal start. 1—Enable fast start.
1—H.323 only	0/1—Disable/enable h245 tunneling.
2	0—Use the dynamic payload type 126/127 as the RTP payload type (fax pass-through mode) for G.711 μ -law/G.711 A-law. 1—Use the standard payload type 0/8 as the RTP payload type (fax pass-through mode) for G.711 μ -law/G.711 A-law.
3—H.323 only	0/1—Disable/enable the requirement for the alternate gatekeeper to register.
4—H.323 only	0—Denotes a non-Cisco CallManager environment. 1—Enable the Cisco ATA to operate in a Cisco CallManager environment.
5—H.323 only	0/1—Enable/disable two-way cut-through of voice path before receiving CONNECT message.
6—H.323 only	0/1—Disable/enable using the Progress Indicator to determine if ringback is supplied by the far end with RTP.
7	0/1—Disable/enable fax pass-through redundancy.
8-12	Specifies the fax pass-through NSE payload type. The value is the offset to the NSE payload base number of 96. The valid range is 0-23; the default is 4. For example, if the offset is 4, the NSE payload type is 100.
13	0—Use G.711 μ -law for fax pass-through codec. 1—Use G.711A-law for fax pass-through codec.
14-15	0—Use fax pass-through. 1—Use codec negotiation in sending fax. 2—Reserved. 3—Reserved.
16—SIP only	0/1—Disable/enable SIP to remove the registration before adding a new one.

Table 5-4 ConnectMode Parameter Bit Definitions (continued)

Bit Number	Definition
17—SIP only	0/1—Disable/enable call forwarding performed by the Cisco ATA. In SIP, call forwarding can be performed locally by the Cisco ATA or it can be performed by the SIP proxy. If this bit is disabled, the Cisco ATA forwards the entire dial string, including service activation code, to the SIP proxy for processing.
18—SIP only	0/1—Disable/enable SIP call return performed by the Cisco ATA.
19	0/1—Disable/enable the Cisco ATA to send a ringback tone to the caller.
20—SIP only	0/1—Disable/enable SIP to perform action=proxy in a REGISTER message.
21—SIP only	0/1—Disable/enable SIP to perform action=redirect in a REGISTER message.
22—SIP only	<p>0/1—Disable/enable SIP to process a <i>received=</i> tag in the VIA header to extract the external IP addresses used by the Network Address Translation (NAT) router.</p> <p>When the Cisco ATA is operating behind a NAT, the NATIP parameter must be set to the external IP address of the NAT router. This allows the correct IP address to be placed in the Contact and SDP headers.</p> <p>In release 2.14 or later, you may leave the NAT IP address at the default value of "0" or "0.0.0.0" and let the ATA automatically scan the Via header for a "received=" parameter. The parameter, if present, would indicate that the Cisco ATA is operating behind a firewall.</p> <p>The Cisco ATA proceeds as follows:</p> <ol style="list-style-type: none"> 1. If the "received=" parameter is in an INVITE response, the current INVITE is canceled and a new INVITE is sent with the new IP address extracted from the "received=<NAT IP address>" parameter in the Contact and SDP headers. <p>In addition, the Cisco ATA will cancel all previous registrations and re-register with the new IP address in the Contact header. This step is performed only if registration is currently in an idle state.</p> <ol style="list-style-type: none"> 2. If the "received=" parameter is in a REGISTER response as a result of a REGISTER command, the Cisco ATA will cancel all previous registrations and re-register with the new IP address extracted from the "received=<NAT IP address>" parameter in the Contact header. <div style="margin-top: 10px;">  <p>Note For the Cisco ATA to automatically detect its presence behind a NAT, the SIP proxy server or remote user agent server <i>must</i> include the "received=" parameter in the Via header in the responses to the Cisco ATA if the proxy detects that the source address and port do not match those in the Via header.</p> </div>
23	0/1—Disable/enable the end user to specify the default call waiting state for every call. This can be done on a permanent basis.
24	0/1—Disable/enable the mixing of audio and call waiting tone during a call.
25—SIP only	0/1—Disable/enable DNS lookup of hostname "From" header hostname for call return.
26 to 31	Reserved.

**Note**

You cannot simultaneously set bits 20 and 21 to 1. Also, if you set both these bits 0, the action parameter is not included in the REGISTER message, forcing the proxy server to perform the next step in the call process.

AutMethod

Description

This parameter is not used for SIP.

TimeZone

Description

This parameter is the timezone offset from Greenwich Mean Time (GMT) for time-stamping incoming calls with local time (to use for Caller ID display, for example).

Local time is generated by the following formula:

- Local Time=GMT + TimeZone, if TimeZone <= 12
- Local Time=GMT + TimeZone - 25, if TimeZone > 12

Value Type

Integer

Range

0-24

Default

17

Voice Configuration Menu Access Code

302

NTPIP

Description

This parameter is the NTP IP address, required if DHCP server does not provide one.

The Cisco ATA requires an NTP Server from which to obtain Coordinated Universal Time (UTC) to time-stamp incoming calls (H.323 and SIP) to drive an external Caller-ID device.

DHCP may also supply a NTP server. If NTPIP is specified, it overwrites the value supplied by DHCP. NTPIP is ignored if its value is 0 or 0.0.0.0.

The user *must not* specify a port parameter. The Cisco ATA uses the default NTP port only.

Value Type

IP address

Default

0.0.0.0

Voice Configuration Menu Access Code

141

AltNTPIP

Description

This parameter is the alternate NTP IP address, if you want redundancy. You can set this parameter to 0 or point to the same NTPIP if only one NTP server exists.

Value Type

IP address

Default

0.0.0.0

Voice Configuration Menu Access Code

142

DNS1IP

Description

This parameter is the primary domain name server (DNS) IP address, if the DHCP server does not provide one. If DHCP provides DNS, DNS1IP and DNS2IP (if they are non-zero) overwrite the DHCP-supplied values. The user *must not* specify a port parameter. The Cisco ATA uses the default DNS port only.

Value Type

IP address

Default

0.0.0.0

Voice Configuration Menu Access Code

916

DNS2IP

Description

This parameter is the secondary domain name server (DNS) IP address, if the DHCP server does not provide one. If DHCP provides DNS, DNS1IP and DNS2IP (if they are non-zero) overwrite the DHCP-supplied values. The user *must not* specify a port parameter. The Cisco ATA uses the default DNS port only.

Value Type

IP address

Default

0.0.0.0

Voice Configuration Menu Access Code

917

UDPTOS

Description

This parameter specifies the IP precedence (ToS bit) of UDP packets. Set the lower eight bits only, as follows:

- Bits 0-1: Unused
- Bit 2: Reliability bit—1=request high reliability
- Bit 3: Throughput bit—1=request high throughput
- Bit 4: Delay bit—1=request low delay
- Bits 5-7: Specify datagram precedence. Values range from 0 (normal precedence) to 7 (network control).

Value Type

Bitmap

Default

0xB8

Voice Configuration Menu Access Code

255

SigTimer

Description

This parameter controls various timeout values. Table 5-5 on page 5-33 contains bit definitions of this parameter.

Value Type

Bitmap

Default

0x01418564

Voice Configuration Menu Access Code

318

Table 5-5 SigTimer Parameter Bit Definitions

Bit Number	Definition
0-7	Call waiting period—The period between each burst of call-waiting tone. Range: 0 to 255 in 0.1 seconds Default: 100 (0x64=100 seconds)
8-13	Reorder delay—The delay in playing the reorder (fast busy) tone after the far-end caller hangs up. Range: 0 to 62 in seconds Default—5 (seconds) 63—Never play the reorder tone.
14-19	Ring timeout—When a call is not answered, this is the amount of time after which Cisco ATA rejects the incoming call. Range—0 to 63 in 10 seconds Default—6 (60 seconds) 0—Never times out
20-25	No-answer timeout—The time to declare no answer and initiate call forwarding on no answer (used in SIP only) Range—0 to 63 in seconds Default—20 (0x14=20 seconds)
26-27	Minimum hook flash time—The minimum on-hook time required for hook flash event. Range: 0 to 3 Default: 0 (60 ms) Other possible values: 1=100 ms, 2=200 ms, 3=300 ms.
28-31	Maximum hook flash time—The maximum on-hook time allowed for hook flash event. Range: 0 to 15 Default: 0 (1000 ms) Other possible values: 1=100 ms, 2=200 ms, 3=300 ms, 4=400 ms, 5=500 ms, 6=600 ms, 7=700 ms, 8=800 ms, 9=900 ms, 10=1000 ms, 11=1100 ms, 12=1200 ms, 13=1300 ms, 14=1400 ms, 15=1500 ms.

OpFlags

Description

This parameter enables/disables various operational features.

See Table 5-6 on page 5-34 for bit definitions of this parameter.

Value Type

Bitmap

Default

0x2

Voice Configuration Menu Access Code

323

Table 5-6 OpFlags Parameter Operational Features to Turn On or Off

Bit Number	Definition
0	If Bit 0 = 0, the TFTP configuration filename supplied by the DHCP server overwrites the default filename for each Cisco ATA. If Bit 0 = 1, the default Cisco ATA filename is always used.
1	If Bit 1 = 0, the Cisco ATA probes the static network router during the power-up process. If Bit 1 = 1, static network router probing is disabled.
2	Reserved.
3	If Bit 3=1, the Cisco ATA does not request DHCP option 150 in the DHCP discovery message; some DHCP server do not respond if option 150 is requested.
4	If Bit 4 = 1, the Cisco ATA uses the VLAN ID specified in the VLANSetting parameter for VLAN IP encapsulation (see the “VLANSetting” section on page 5-35).
5	If Bit 5=1, the Cisco ATA does not use VLAN IP encapsulation.
6	If Bit 6=1, the Cisco ATA does not perform CDP discovery.
7	If Bit 7=1, the Cisco ATA does not allow web configuration. Once the web server is disabled, you must configure the Cisco ATA with the TFTP or voice configuration menu methods. Examples 1. If the existing OpFlags value is 0x2, select menu option 323 from the voice configuration menu and enter the value 130 (0x82). This disables web configuration. If you later attempt to access the Cisco ATA web configuration page, the following error messages will be displayed. <ul style="list-style-type: none"> - Netscape: The document contained no data. Try again later, or contact the server's administrator. - Internet Explorer: The page cannot be displayed. 2. If the existing OpFlags value is 0x82, select menu option 323 from the voice configuration menu and enter the value 2 (0x2). This disables web configuration.
8	If Bit 8=1, the Cisco ATA does not allow HTTP refresh access with the http://ip/refresh command.
9	If Bit 9=1, the Cisco ATA does not allow HTTP reset access with the http://ip/reset command.

Table 5-6 OpFlags Parameter Operational Features to Turn On or Off (continued)

Bit Number	Definition
10	Reserved.
11	If Bit 11=0, the Cisco ATA requests the device hostname from the DHCP server. If Bit 11=1, the Cisco ATA uses the device hostname that is specified in DHCP option 12.
12-27	Reserved.
28-31	To configure the Cisco ATA to prompt the user for the UIPassword when the user attempts to perform a factory reset or upgrade using the voice configuration menu, configure bits 28 to 31 with the value of 6. Any other value for these bits means that the Cisco ATA will not prompt the user for the UIPassword in these cases.

VLANSetting

Description

This parameter is for firmware version 2.15 and 2.14ms, and above.

Bitmap definitions are as follows for the VLANSetting parameter:

- 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 6-17—Reserved.
- Bits 18-29—User-specified 802.1Q VLAN ID.
- Bits 30-31—Reserved.

Value Type

Bitmap

Default

0x0000002b

Voice Configuration Menu Access Code

324

Optional Feature Parameters

This section describes the following parameters, which are located in the wheat-colored portion of the Cisco ATA Web Configuration Page:

- NPrintf, page 5-36
- TraceFlags, page 5-36
- RingOnOffTime, page 5-37
- IPDialPlan, page 5-38

- DialPlan, page 5-38
- Call-Progress Tone Parameters, page 5-42
- CallCmd, page 5-47

NPrintf

Description

Use this parameter to specify the IP address and port of a host to which all Cisco ATA debug messages are sent. The program *prserv.exe*, which comes bundled with the Cisco ATA software, is needed to capture the debug information.

Syntax

<HOST_IP>, <HOST_PORT>

Example

If the program *prserv.exe* is running on a host with IP address 192.168.2.170 and listening port 9001, set NPrintf to 192.168.2.170.9001. This causes the Cisco ATA to send all debug traces to that IP address.

Value Type

Extended IP address

Default

0

Voice Configuration Menu Access Code

81

TraceFlags

Description

Use this parameter to turn on specific trace features for diagnostic use. Bit values are as follows:

- Bits 0 to 1:
 - 0 (default) is for simple debug messages.
 - 1 is for detailed debug messages.
 - 2 and 3 are reserved.
- Bits 2-7—Reserved
- Bit 8—RTP statistics log (values **0/1** to disable/enable with default of **0**) has the following format:
 Recv[channel number]: <call duration in seconds> <number of recv packets>
 <number of recv octets> <number of late packets>
 <number of lost packets> <average network jitter in 1/8 ms>
 <counts in speeding up local clock (adjustment for 10 ms each time)>
 <counts in slowing down local clock (adjustment for 10 ms each time)>



Note Bit 8 is not used at this time.

- Bits 9 to 31—Reserved.

Value Type

Bitmap

Default

0x00000000

Voice Configuration Menu Access Code

313

RingOnOffTime

Description

This parameter specifies the ringer cadence pattern, expressed as a triplet of integers “a,b, and c”.

- a—Number of seconds to turn the ring ON.
- b—Number of seconds to turn the ring OFF.
- c—The ring frequency, fixed at 25.

Value Type

List of three integer values, separated by commas

Range

1-65535

Default

2, 4, 25

Recommended Values:

- United States —2,4,25
- Sweden — 1,5,25

Voice Configuration Menu Access Code

929

IPDialPlan

Description

This Iparameter allows for detection of IP-like destination address in DialPlan. Three values are valid:

- 0—String is dialed as is and not treated as an IP address.
- 1—When the Cisco ATA detects two asterisks (**), IPDialPlan takes over. The user enters the pound (#) key to terminate the digit collection, and the interdigit timeout default is not used.
- 2—When IPDialPlan is set to 2, three asterisks (***) are required for IPDialPlan to take effect.

All other values are currently undefined.

Value Type

Integer

Range

0, 1 or 2

Default

1

Voice Configuration Menu Access Code

310

DialPlan

Description

The programmable dial plan is designed for the service provider to customize the behavior of the Cisco ATA for collecting and sending dialed digits. The dial plan allows the Cisco ATA user to specify the events that trigger the sending of dialed digits. These events include the following:

- The termination character has been entered.
- The specified dial string pattern has been accumulated.
- The specified number of dialed digits has been accumulated.
- The specified inter-digit timer has expired.

Value Type

Alphanumeric string

Range

Maximum number of characters is 199.

Default

*St4-|#St4-|911|1>#t8.r9t2-|0>#t811.rat4-|^1t4>#.-

Voice Configuration Menu Access Code

926

Additional DialPlan Information

The DialPlan section contains the following additional topics that describe commands and rules for creating your own dial plan:

- About Dial Plan Commands, page 5-39
- Dial Plan Blocking (In Rule), page 5-41
- 'H' Rule to Support Hot/Warm Line, page 5-41
- 'P' Rule to Support Dial Prefix, page 5-42

About Dial Plan Commands

The following list contains rules for Cisco ATA dial plans:

- `.` —Wildcard, match any digit entered.
- `-` —Additional digits can be entered. This command can be used only at the end of a dial plan rule (for example, 1408t5- is legal usage of the `-` command, but 1408t5-3... is illegal).
- `>#`—Defines the `#` character as a termination character. When the termination character is entered, the dial string is automatically sent. The termination character can be entered only after at least one user-entered digit matches a dial plan rule. Alternatively, the command `>*` can be used to define `*` as the termination character.
- `tn`— Defines the timeout value **n**, in the unit of seconds, for the interdigit timer. Valid values are 0-9 and a-z, where a-z indicates a range of 10 to 36.
- `rn`—Repeat the last pattern **n** times, where **n** is 0-9 or a-z. The values a-z indicate a range of 10 to 36. Use the repeat modifier to specify more rules in less space.



Note

The commands `>#` and `tn` are modifiers, not patterns, and are ignored by the `rn` command.

- `|`—Used to separate multiple dial plan rules.
- `^`—Logical not. Match any character except the character immediately following the `^` command.
- `S`—Seize rule matching. If a dial plan rule matches the sequence of digits entered by the user to this point, and the modifier `S` is the next command in the dial plan rule, all other rules are negated for the remainder of the call (for example, a dial plan beginning with `*S` will be the only one in effect if the user first enters the `*` key).



Note

All rules apply in the order listed (whichever rule is completely matched first will immediately send the dial string).



Note

No syntax check is performed by the actual implementation. The administrator has the responsibility of making sure that the dial plan is syntactically valid.

Dial Plan Example 1 (Default Dial Plan)

The following dial plan:

```
*St4- | #St4- | 911 | 1>#t8.r9t2- | 0>#t811.rat4- | ^1t4>#.-
```

consists of the following rules:

- ***St4**—If the first digit entered is *, all other dial plan rules are voided. Additional digits can be entered after the initial * digit, and the timeout before automatic dial string send is four seconds.
- **#St4**—Same as above, except with # as the initial digit entered.
- **911**—If the dial string 911 is entered, send it immediately.
- **1>#t8.r9t2**—If the first digit entered is 1, the timeout before automatic send is eight seconds. The terminating character # can be entered at any time to manually send the dial string. After the 11th digit is entered, the timeout before an automatic send changes to two seconds. The user can enter more digits until the dial string is sent by the timeout or by the user entering the # character.
- **0>#t811.rat4**—If the first digit entered is 0, the timeout before automatic send is eight seconds, and the terminating character # can be entered at any time to manually send the dial string. If the first three digits entered are 011, then, after an additional 11 digits are entered, the timeout before an automatic send changes to four seconds. The user can enter more digits until the dial string is sent by the timeout or by the user entering the # character.
- **^1t4>#**—If the first digit entered is anything other than 1, the timeout before an automatic send is four seconds. The terminating character # can be entered at any time to manually send the dial string. The user can enter more digits until the dial string is sent by the timeout or by the user entering the # character.

Dial Plan Example 2

The following dial plans:

```
.t7>#. . . . .t4- | 911 | 1t7>#. . . . .t1- | 0t4>#.t7-
```

or

```
.t7>#r6t4- | 911 | 1t7>#.r9t1- | 0t4>#.t7-
```

consist of the following rules:

- **.t7>#r6t4-**—You must enter at least one digit. After the first digit is entered and matched by the dial plan, the timeout before an automatic send is seven seconds, and the terminating character # can be entered at any time to manually send the dial string. After seven digits are entered, the timeout before an automatic send changes to two seconds. The **- symbol** at the end of the rule allows further digits to be entered until the dial string is sent by the timeout or the user entering the # character.
- **911**—If the dial string 911 is entered, send this string immediately.
- **1t7>#.r9t1**—If the first digit entered is 1, the timeout before an automatic send is seven seconds, and the terminating character # can be entered at any time to manually send the dial string. After the 11th digit is entered, the timeout before an automatic send changes to one second. The user can enter more digits until the dial string is sent by the timeout or by the user entering the # character.
- **0t4>#.t7**—If the first digit entered is 0, the timeout before an automatic send is four seconds, and the terminating character # can be entered at any time to manually send the dial string. After the second digit is entered, the timeout before an automatic send changes to seven seconds. The user can enter more digits until the dial string is sent by the timeout or by the user entering the # character.

Dial Plan Blocking (*In* Rule)

Dial plan blocking can be used to reduce the occurrences of invalid dialed digits being sent and can prevent the dialed string of a specified pattern from being sent. By adding dial plan blocking, dialed digits are discarded after the interdigit timer expires unless one of the specified matching rules is met.

In addition, the default nine-second global interdigit timeout value is also modified with the value specified in the dial plan blocking command:

In

where **n** specifies the global interdigit timeout and the valid values are 1-9 and a-z (10-35).

For example, to enter an interdigit timeout of 12 seconds and discard dialed digits unless 911 is entered, you would use the following command:

Ic1 911

Specifying your own interdigit timeout also changes the behavior of the dial plan so that the entire dial string, rather than being sent at timeout, is sent only as a result of a matching rule or time intended by a matching rule.

'H' Rule to Support Hot/Warm Line

Hotline/Warmline, also known as Private Line Automatic Ringdown (PLAR), is a line used for priority telephone service. If the Hotline feature is configured, the Cisco ATA immediately dials a pre-configured number as soon as the handset goes off hook. If the Warmline feature is configured, the Cisco ATA dials a pre-configured number if no digits were entered before the specified timer value expired when the handset went offhook.

Syntax

Hdnnnn

where **d** is a delay-in-seconds parameter 0-9,a-z (to support 0 to 35 seconds delay), and **nnnn** is the variable-length phone number to call when no digits are entered for **d** seconds after offhook.

- Example 1: **H05551212** (Hotline configuration; the Cisco ATA immediately dials 555-1212 when the handset goes off hook.)
- Example 2: **H55551212** (Warmline configuration; the Cisco ATA waits for five seconds and dials 555-1212 if no digits were entered when the handset went off hook.)

'P' Rule to Support Dial Prefix

This rule is for automatic pre-pending the dial string as entered by the user with a specified prefix.

Syntax

Ptnnnn

where **t** is a single leading trigger character; if **t** is the *first* entered digit when making a new call, it triggers the prepending of a variable-length prefix (as specified by **nnnn**) in the dial string. The **t** character can take one of the following values:

0-9, *, #, 'n' (= any of 1-9), 'N' (any of 'n' and 0), 'a' (any of 'n', * and #), or 'A' (any of 'a' and 0);

Example:

Pn12345: Prepends 12345 to the dial string when the first entered digit is any of 1-9. The triggered digit is not removed from the dial string.

Call-Progress Tone Parameters

This section contains the following topics:

- List of Call-Progress Tone Parameters, page 5-42
- Tone Parameter Syntax, page 5-42
- How to Calculate Scaling Factors, page 5-43
- Recommended Values, page 5-44
- Specific Call-Progress Tone Parameter Information, page 5-44

List of Call-Progress Tone Parameters

The following list contains the names of the call-progress tone parameters:

- DialTone
- BusyTone
- ReorderTone
- RingBackTone
- CallWaitTone
- AlertTone

Tone Parameter Syntax

Each tone is specified by nine intergers, as follows:

ntone, freq0, freq1, level0, level1, steady, on-time, off-time, total-tone-time

- **ntone** is the number of frequency components (0, 1 or 2).
- **freq[0]** (Hz) is the transformed frequency of the first frequency component (-32768 to 32767).

**Note**

Only positive values can be configured to the Cisco ATA 186. For negative values, use the 16-bit 2's-complement value. For example, enter -1 as 65535 or 0xffff.

- **freq[1]** is the transformed frequency of the second frequency component (-32768 to 32767).
- **level[0]** is the transformed amplitude of the first frequency component (-32768 to 32767).
- **level[1]** is the transformed amplitude of the second frequency component (-32768 to 32767).
- **steady** controls whether the tone is constant or intermittent. A value of 1 indicates a steady tone and causes the Cisco ATA to ignore the on-time and off-time parameters. A value of 0 indicates an on/off tone pattern and causes the Cisco ATA to use the on-time and off-time parameters.
- **on-time** controls the length of time the tone is heard in milliseconds (ms) expressed as an integer from 0 to 0xffff sample at 8000 samples/second.
- **off-time** controls the length of time between audible tones in milliseconds (ms) expressed as an integer from 0 to 0xffff sample at 8000 samples/second.
- **total-tone-time** controls the length of time the tone is audible (0 to 0xffff). If this value is set to 0, the tone will play until another call event stops the tone. For DialTone, BusyTone, ReorderTone, and RingBackTone, the configurable value is the number of 10 ms (100 = 1 second) units.

For the other tones, the value is the number of samples at 8000 samples/second, where the following information applies:

- Frequency ranges from 0 to 4000 (Hz)
- Transformed Frequency = $32767 \cdot \cos(2\pi \cdot \text{Frequency}/8000)$
- Amplitude ranges from 0 to 32767
- Transformed Amplitude = $A \cdot 32767 \cdot \sin(2\pi \cdot \text{Frequency}/8000)$

The scaling factor *A* determines the volume level of the tone. To calculate scaling factors, see the “How to Calculate Scaling Factors” section on page 5-43.

**Note**

All tones are persistent (until the Cisco ATA changes state) except for the call-waiting tone and the confirm tone. The call-waiting tone, however, repeats automatically once every 10 seconds while the call-waiting condition exists.

How to Calculate Scaling Factors

Use the following formula to calculate the scaling factor *A*:

$$A = 0.5 * 10^{((k+10-(n-1)*3)/20)}$$

In this formulas, *k* is the desirable volume in dBm; *n* is the number of frequency components. The ^ symbol means *to the order of*.

Example

If a one-frequency component of -20 dBm volume level is desirable, then:

$$A = 0.5 * 10^{((-20+10)/20)} = 0.16$$

Recommended Values

The following settings are recommended for the US:

- DialTone = "2,31538,30831,3100,3885,1,0,0,1000" (approximately -10 dBm)
- BusyTone = "2,30467,28959,1191,1513,0,4000,4000,0" (approximately -21 dBm)
- ReorderTone = "2,30467,28959,1191,1513,0,2000,2000,0" (approximately -21 dBm)
- RingBackTone = "2,30831,30467,1943,2111,0,16000,32000,0" (approximately -16 dBm)
- CallWaitTone = "1,30831,0,5493,0,0,2400,2400,4800" (approximately -10 dBm)
- AlertTone = "1,30467,0,5970,0,0,480,480,1920" (approximately -10 dBm)

The following settings are recommended for Sweden:

- DialTone = "1,30959,0,4253,0, 1, 0, 0,1500" (approximately -5 dBm)
- BusyTone = "1,30959,0,2392,0, 0, 2000, 2000,0" (approximately -10 dBm)
- ReorderTone = "1,30959,0,2392,0, 0, 2000, 6000,0" (approximately -10 dBm)
- RingBackTone = "1,30959,0,2392,0, 0, 8000, 40000,0" (approximately -10 dBm)
- CallWaitTone = "1,30959,0,2392,0, 0, 1600, 4000,11200" (approximately -10 dBm)
- AlertTone = "1,30959,0,2392,0, 0, 480, 480,1920" (approximately -10 dBm)

Specific Call-Progress Tone Parameter Information

Brief descriptions, and lists of default values and the voice configuration menu code for each Cisco ATA tone parameter, are described in the following sections:

- DialTone, page 5-44
- BusyTone, page 5-45
- ReorderTone, page 5-45
- RingbackTone, page 5-46
- CallWaitTone, page 5-46
- AlertTone, page 5-47

DialTone

Description

The Cisco ATA plays the dial tone when it is ready to accept the first digit of a remote address to make an outgoing call.

Default values for the nine-integer array

- ntone—2
- freq0—31538
- freq1—30831
- level0—1380
- level1—1740
- steady—1

- on-time—0
- off-time—0
- total time to play tone—1000

Voice Configuration Menu Access Code

920

BusyTone**Description**

The Cisco ATA plays the busy tone when the callee is busy.

Default values for the nine-integer array

- ntone—2
- freq0—30467
- freq1—28959
- level0—1191
- level1—1513
- steady—0
- on-time—4000
- off-time—4000
- total time to play tone—0

Voice Configuration Menu Access Code

921

ReorderTone**Description**

The Cisco ATA plays the reorder tone (also known as congestion tone) if the outgoing call failed for reasons other than busy.

Default values for the nine-integer array

- ntone—2
- freq0—30467
- freq1—28959
- level0—1191
- level1—1513
- steady—0
- on-time—2000

- off-time—2000
- total time to play tone—0

Voice Configuration Menu Access Code

922

RingbackTone**Description**

The Cisco ATA plays the ring-back tone when the callee is being alerted by the called device.

Default values for the nine-integer array

- ntone—2
- freq0—30831
- freq1—30467
- level0—1943
- level1—2111
- steady—0
- on-time—16000
- off-time—32000
- total time to play tone—0

Voice Configuration Menu Access Code

923

CallWaitTone**Description**

The Cisco ATA plays the call-waiting tone when an incoming call arrives while the user is connected to another party.

Default values for the nine-integer array

- ntone—1
- freq0—30831
- freq1—0
- level0—5493
- level1—0
- steady—0
- on-time—2400

- off-time—2400
- total time to play tone—4800

Voice Configuration Menu Access Code

924

AlertTone**Description**

The Cisco ATA plays the alert tone to prompt the user to enter a phone number when invoking a supplementary service, such as call-forwarding, or blind transfer.

Default values for the nine-integer array

- ntone—1
- freq0—30467
- freq1—0
- level0—5970
- level1—0
- steady—0
- on-time—480
- off-time—480
- total time to play tone—1920

Voice Configuration Menu Access Code

925

CallCmd**Description**

Command table that controls call commands such as turning on/off caller ID.

For detailed information on the CallCmd parameter, see Chapter 6, “Call Commands.”

Value Type

Alphanumeric string

Range

Maximum of 248 characters

Default

- US command table:

CallCmd:Af;AH;BS;NA;CS;NA;Df;EB;Ff;EP;Kf;EFh;HQ;Jf;AFh;HQ;I*67;gA*82;fA#90v#;OI;H#72v#;bA#74v#;cA#75v#;dA#73;eA*67;gA*82;fA*70;iA*69;DA*99;xA;Uh;GQ;

- Sweden command table:

CallCmd:BS;NA;CS;NA;Df;EB;Ff0;ARf1;HPf2;EPf3;AP;Kf1;HFf2;EFf3;AFf4;HQ;Jf1;HFf2;EFf3;AFf4;HQ;Af4;HQ;I*31#;gA#31#;gA*90*v#;OI;H*21*v#;bA*61*v#;dA*67*v#;cA#21#;eA#61#;eA#67#;eA*31#;gA#31#;gA*43#;hA#43#;iA*69#;DA*99#;xA

Voice Configuration Menu Access Code

930



Call Commands

This section provides detailed information on call commands for the Cisco ATA:

- Call Command Structure, page 6-1
- Syntax, page 6-2
- Call Command Example, page 6-5
- Call Command Behavior, page 6-7

Service providers can offer many supplementary services, which can be activated, configured, or deactivated in more than one way. The CallCmd parameter allows you to define the behavior of supplementary services that the Cisco ATA supports.



Note

The term *Cisco ATA* refers to both the Cisco ATA 186 and the Cisco ATA 188, unless otherwise stated.



Note

This section contains call command information for the United States and Sweden. For information about other countries, contact the Cisco equipment provider for a specific country.

Call Command Structure

The entry in the CallCmd field is a character string composed of a sequence of instructions, which consist of a combination of three elements:

- **Context**—The Cisco ATA supplementary service operation is dependent upon a state and transition process. For example, the most common state is IDLE, in which the Cisco ATA is on-hook, waiting for an incoming call. Picking up the telephone handset causes the Cisco ATA to transition to the PREDIAL state, in which the user hears a dial tone and the Cisco ATA is waiting to detect DTMF digits. The Context portion of a Call Command string specifies the state for which the commands are defined.
- **Input-Sequence**—The input sequence is simply the input from the user, a combination of hook-flash and DTMF digits.
- **Action**—This specifies the action taken by the Cisco ATA. The action depends on the Input-Sequence that the user enters and the Context in which it is entered.

Syntax

The **CallCmd** string has the following structure:

Context-Identifier Command . . . Command; . . . Context-Identifier Command;

- Table 6-1 provides a list of Context-Identifiers, which show the state of the Cisco ATA.
- **Command** consists of the following items:

Input-Sequence; Action-Identifier-1 Action-Identifier-2 [Input-Sequence]

- **Input Sequence** consists of one or more characters from the set shown in Table 6-2.
- Table 6-3 provides a list of Action Identifiers. **Action-Identifier-1** is for the first thread of a call; **Action-Identifier-2** is for the second thread of a call. Each Action Identifier is one character.

Each Context-Identifier is followed by one or more commands to allow a variable number of actions to be triggered by relevant user input commands for any state. Each command is composed of an Input-Sequence that the user enters when the Cisco ATA is in a given state and two Action-Identifier characters which define the action that the Cisco ATA performs in response to the Context-Identifier and Input-Sequence. If the Cisco ATA takes only one action, one of the two Action-Identifier characters is a null action.

Example 6-1 Syntax Example Using One Command

```
Af;AH;
```

In this simple example, the first “A” is the Context-Identifier, which means the Cisco ATA is in the CONFERENCE state, as shown in Table 6-1. The “f” is the input sequence, which is hook-flash, as shown in Table 6-2. Following the semicolon, the two action identifiers are “A” and “H”. These identifiers mean “NONE” and “Disconnect the call,” respectively, as shown in Table 6-3. Based on these action identifiers, the Cisco ATA disconnects the most recent callee, and remains connected to the first party. The state of the Cisco ATA becomes CONNECTED. Table 6-4 explains more about the various states of the Cisco ATA.

Example 6-2 Syntax Example Using Two Commands

```
CN;CAf;OF;
```

In this example, the first “C” is the Context Identifier, which means the Cisco ATA is in the PREDIAL_HOLDING state, as shown in Table 6-1. The “N” is the first input sequence, which is any part of the set of digits 0|1|2|3|4|5|6|7|8|9, as shown in Table 6-2. Following the first semicolon, the two action identifiers are “C” and “A”, which mean “Continue to Dial” and “NONE,” respectively, as shown in Table 6-3.

Following this pair of action identifiers is another input sequence, “f”, which means hook-flash, as shown in Table 6-2. Next is the semicolon, always required after the input sequence, followed by the corresponding action pair, “O” and “F”. These identifiers mean “Release the Call” and “Retrieve the Call,” respectively, as shown in Table 6-3.

Context-Identifiers

Table 6-1 *Context-Identifiers*

Identifier	Context (State of Cisco ATA)
A	CONFERENCE
B	PREDIAL
C	PREDIAL_HOLDING
D	CONNECTED
E	CONNECTED_HOLDING
F	CONNECTED_ALERTING
G	HOLDING
H	CONFIGURING
I	CONFIGURING_HOLDING
J	3WAYCALLING
K	CALLWAITING
L	IDLE
M	RINGING
N	DIALING
O	CALLING
P	Reserved (ANSWERING)
Q	Reserved (CANCELING)
R	Reserved (DISCONNECTING)
S	WAITHOOK
T	DIALING_HOLDING
U	CALLING_HOLDING
V	Reserved (ANSWERING_HOLDING)
W	Reserved (HOLDING_HOLDING)
X	Reserved (CANCELING_HOLDING)
Y	Reserved (DISCONNECTING_HOLDING)
Z	Reserved (HOLDING_ALERTING)
a	WAITHOOK_ALERTING
b	WAITHOOK_HOLDING

Input Sequence Identifiers

Table 6-2 *Input Sequence Identifiers*

Identifier	Input Sequence
0-9,#*	DTMF digits
f	hook flash
o	off-hook
@	anytime; for example, @f means anytime hook-flash occurs
h	on-hook
S	# *
N	0 1 2 3 4 5 6 7 8 9
D	NIS
v	a variable number (1 or more) of characters from the above list. It must be followed by a character which acts as the terminator of this variable part.

Action Identifiers

Table 6-3 *Action Identifiers*

Identifier	Action
A	NONE
B	Seizure (User intends to dial or configure)
C	Continue to dial
D	Call Return
E	Hold the active call
F	Retrieve the waiting call
G	Cancel the call attempt
H	Disconnect the call
I	Blind transfer the call to the number
N	Go to configuration mode
O	Release the call
P	Answer the incoming call
Q	Transfer with consultation
R	Say busy to the caller
a	None
b	Forward all calls to the given number

Table 6-3 Action Identifiers (continued)

c	Forward on busy to the given number
d	Forward on no answer to the given number
e	Cancel call forward
f	CLIP for the next call
g	CLIR for the next call
h	Enable Call Waiting for the next call
i	Disable Call Waiting for the next call
x	Enable Fax Mode for the next call
y	Disable Fax Mode for the next call

Call Command Example

In addition to call commands that you configure, the Cisco ATA has a default list of call commands to handle common call scenarios. Configured call commands overwrite default call commands. If any Context-Identifier or Input-Sequence elements appear in both the default Call Command string and the manually entered string, the manually entered value takes precedence.

The following string shows a sample Call Command:

```
Bf;BAN;CA;CN;CAf;OF;Df;EB;I@f;OF;H@f;OA;Lo;BAf;BA;Mo;PA;ND;CAf;OA;Of;GA;Pf;HA;Qf;OA;Rf;OA;Sf;OA;TD;CAf;OF;Uf;GF;Vf;HF;Wf;FF;Xf;Af;Yf;Af;Zf;AP;bf;OF;af;OP;
```

In this section, the Call Command string is broken down into its components as follows:

```
Call Command Fragment;
Context-Identifier
    Input-Sequence1; Action1 Action2;
    (optional) Input-Sequence2; Action1 Action2;
```



Note If you use a second input sequence, this sequence follows the Action Identifier pair without a separating semicolon.

Refer to the preceding tables to determine the meanings of the identifiers.

Example 6-3 Call Command String

```
Bf;BAN;CA;
    Predial
        hook-flash; Seizure NONE
        0|1|...|9; Continue-to-dial NONE;
CN;CAf;OF;
    Predial_Holding
        0|1|...|9; Continue-to-dial NONE
        hook-flash; Release-the-call Retrieve-the-waiting-call;
Df;EB;
    Connected
        hook-flash; Hold-the-active-call Seizure;
I@f;OF;
    Configuring_Holding
        hook-flash (at any time); Release-the-call Retrieve-the-waiting-call;
H@f;OA;
```

```

Configuring
    hook-flash (at any time); Release-the-call NONE;
Lo;BAf;BA;
    Idle
        off-hook; Seizure NONE;
        hook-flash; Seizure NONE;
Mo;PA;
    Ringing
        off-hook; Answer-the-incoming-call NONE;
ND;CAf;OA
    Dialing
        0|1|...|9|#|*; Continue-to-dial NONE
        hook-flash; Release-the-call NONE;
Of;GA;
    Calling
        hook-flash; Cancel-the-call-attempt NONE;
Pf;HA;
    Answering
        hook-flash; Disconnect-the-call NONE;
Qf;OA;
    Canceling
        hook-flash; Release-the-call NONE;
Rf;OA;
    Disconnecting
        hook-flash; Release-the-call NONE;
Sf;OA;
    Waithook
        hook-flash; Release-the-call NONE;
TD;CAf;OF;
    Dialing_Holding
        0|1|...|9|#|*; Continue-to-dial NONE;
        hook-flash; Release-the-call NONE;
Uf;GF;
    Calling_Holding
        hook-flash; Cancel-the-call-attempt Retrieve-the-waiting-call;
Vf;HF;
    Answering_Holding
        hook-flash; Disconnect-the-call Retrieve-the-waiting-call;
Wf;FF;
    Holding_Holding
        hook-flash; Retrieve-the-waiting-call Retrieve-the-waiting-call;
Xf;AF;
    Canceling_Holding
        hook-flash; NONE Retrieve-the-waiting-call;
Yf;AF;
    Disconnecting_Holding
        hook-flash; NONE Retrieve-the-waiting-call;
Zf;AP;
    Holding_Alerting
        hook-flash; NONE Answering;
bf;OF;
    Waithook_Holding
        hook-flash; Release-the-call Retrieve-the-waiting-call;
af;OP;
    Waithook_Holding
        hook-flash; Release-the-call Answer-the-incoming-call;

```

Call Command Behavior

Table 6-4 summarizes differing Call Command behavior based on the U.S. and Sweden default call commands.

U.S. Call Command Default

Af;AH;BS;NA;CS;NA;Df;EB;Ff;EP;Kf;EFh;HQ;Jf;AFh;HQ;I*67;gA*82;fA#90v#;OI;H#72v#;bA#74v#;cA#75v#;dA#73;eA*67;gA*82;fA*70;iA*69;DA*99;xA;Uh;GQ;Af;AH;

Sweden Call Command Default

BS;NA;CS;NA;Df;EB;Ff0;ARf1;HPf2;EPf3;AP;Kf1;HFf2;EFf3;AFf4;HQ;Jf1;HFf2;EFf3;AFf4;HQ;Af4;HQ;I*31#;gA#31#;gA*90*v#;OI;H*21*v#;bA*61*v#;dA*67*v#;cA#21#;eA#61#;eA#67#;eA*31#;gA#31#;gA*43#;hA#43#;iA*69#;DA*99#;xA;Uh;GQ;

Table Notations

The following notations are used in Table 6-4:

- FE—Far end
- AFE—Active Far End, which is a connected far end that is not placed on hold
- WFE—Waiting Far End, which is a connected far end being placed on hold, or an incoming caller waiting to be answered
- R—Hook Flash
- ONH—On Hook
- OFH—Off Hook
- 0-9,*,#—DTMF digits
- v—a variable length string, usually a phone number, and does not include #
- CWT—call-waiting tone



Note

The notations in Table 6-4 include abbreviations for input sequence behavior. Refer to the tables and syntax examples shown earlier in this section. The Summary of Commands column in Table 6-4 is based on the actual command syntax used in the default Call Command strings for the United States and Sweden.

Table 6-4 Call Command Behavior

Cisco ATA State and its Definition	Summary of Commands (Input Sequence and Actions)
IDLE: Phone is on-hook; Cisco ATA is waiting for incoming call	<ul style="list-style-type: none"> • OFH—Start dial tone and go to PREDIAL state. • New incoming call or a waiting call (started before it enters IDLE)—Start ringing the phone and go to the RINGING state.
PREDIAL: Phone just went off-hook but no DTMF has been entered yet; Cisco ATA plays dial-tone	<p>United States and Sweden:</p> <ul style="list-style-type: none"> • #, *—Stop dial-tone, go to the CONFIG state, and prepare to accept a complete configuration sequence. • 0-9: Stop dial tone, start invoking dial-plan rules, and go to the DIALING state to accept a complete phone number.

Table 6-4 Call Command Behavior (continued)

Cisco ATA State and its Definition	Summary of Commands (Input Sequence and Actions)
DIALING: User is entering phone number, which is parsed with the given dial-plan rules	<ul style="list-style-type: none"> • R—Abort dialing, restart dial tone, and revert to PREDIAL state. • Invalid phone number—Abort dialing, plays fast-busy, and go to WAITHOOK state.
CONFIG: User configuring a supplementary service in the United States	<ul style="list-style-type: none"> • *69—Call Return • #72v#—Forward unconditional to number specified in 'v' (PacBell use 72#). • #73—Cancel any call forwarding (PacBell use 73#). • #74v#—Forward on busy to number specified in 'v' (PacBell does not enable this service from the phone). • #75v#—Forward on no answer to number specified in 'v' (Pac Bell does not enable this service from the phone). • *67—CLIR in the next call (if global profile is CLIP) • *82—CLIP for the next call (if global user profile is CLIR) • *70—Disable call waiting in the next call. • *99—Enable Fax Mode in the next call (non-standard). • Dial-tone—Revert to PREDIAL state. • Any complete configuration sequence—Carry out the configuration command, restart dial-tone, and revert to PREDIAL state.
CONFIG: User configuring a supplementary service in Sweden	<ul style="list-style-type: none"> • *21*v#—Forward unconditionally to number specified in 'v'. • *67*v#—Forward on busy to number specified in 'v'. • *61*v#—Forward on no answer to number specified in 'v'. • #21#—Cancel any call forwarding. • #67#—Cancel any call forwarding. • #61#—Cancel any call forwarding. • #31#—CLIR in the next call. • *31#—CLIR in the next call. • *43#—Enable call waiting in the next call (Sweden allows globally disable call waiting). • #43#—Disable call waiting in the next call. • *69#—Call Return • (non-standard)*99#—Enable Fax Mode in the next call (non-standard). <p>All Regions:</p> <ul style="list-style-type: none"> • R or any unrecognized sequence—Abort configuration, restart dial tone and revert to PREDIAL state. • Any complete configuration sequence—Carry out the configuration command, restart dial tone, and revert to PREDIAL state.
CALLING: Phone number is sent; Cisco ATA is waiting for response from the far end	<ul style="list-style-type: none"> • R—Cancel the outgoing call, restarts dial-tone, and revert to PREDIAL state.

Table 6-4 Call Command Behavior (continued)

Cisco ATA State and its Definition	Summary of Commands (Input Sequence and Actions)
RINGING: Cisco ATA is ringing the phone to alert user of an incoming call	<ul style="list-style-type: none"> • OFH—Stop ringing, answer the call, and go to CONNECTED state.
CONNECTED: The Cisco ATA is connected with one far end party; Cisco ATA may be the caller or the callee	United States and Sweden: <ul style="list-style-type: none"> • R—Hold current call, play dial-tone to dial second number, and go to PREDIAL_HOLDING state.
WAITHOOK: Far end hangs up while in CONNECTED state; Cisco ATA plays fast-busy after five seconds in this state	<ul style="list-style-type: none"> • R—Stop fast-busy, start dial-tone, and go to PREDIAL state.
CONNECTED_ALERTING: Cisco ATA receives another call while in CONNECTED state; Cisco ATA plays Call Waiting tone periodically (every 10 seconds for US; every second for Sweden)	United States: <ul style="list-style-type: none"> • R—Place current call on-hold, answer the waiting call, and go to CALLWAITING state. Sweden: <ul style="list-style-type: none"> • R0—Continue current call, reject the waiting call, and revert to CONNECTED state. • R1—Disconnect current call, answer the waiting call, and go to CONNECTED state. • R2—Place current call on-hold, answer waiting call, and go to CALLWAITING state. • R3—Continue with current call, answer the waiting call and go to CONFERENCE state. All Regions: <ul style="list-style-type: none"> • ONH—Disconnect current call and go to IDLE state (the Cisco ATA then automatically starts ringing the phone, and goes to RINGING state). • AFE hangs up—Go to WAITHOOK_ALERTING state, continue to play CWT. • WFE cancels the call—Stop CWT and revert to CONNECTED state.
CALL WAITING: Cisco ATA is connected to two far end users on the same line; one is in active conversation (the active far end or AFE) while the other is on-hold (the waiting far end or WFE). This state is initially entered when the Cisco ATA is connected to one of the far ends while the other far end calls into the Cisco ATA.	United States: <ul style="list-style-type: none"> • R—Place the AFE on-hold and retrieve the WFE. • ONH—Transfer the WFE to the AFE, drop out of the call, and go to PREDIAL state. Sweden: <ul style="list-style-type: none"> • R1—Disconnect current call, answer the waiting call, and go to CONNECTED state. • R2—Place the AFE on-hold and retrieve the WFE. • R3—Retrieve the WFE, and go to CONFERENCE state. • R4—Transfer the WFE to the AFE, drop out of the call, and go to PREDIAL state.

Table 6-4 Call Command Behavior (continued)

Cisco ATA State and its Definition	Summary of Commands (Input Sequence and Actions)
3WAYCALLING: Cisco ATA is connected to two far end users on the same line; one of them is in active conversation (the active far end or AFE) while the other is on-hold (the waiting far end or WFE). This state is initially entered when the Cisco ATA is connected to one of the far ends, then places this far end on hold and calls the second far end.	United States: <ul style="list-style-type: none"> • R—Retrieve the WFE and go to CONFERENCE state. • ONH—Transfer the WFE to the AFE, drop out of the call, and go to PREDIAL state. Sweden: <ul style="list-style-type: none"> • Same as for CALLWAITING state
CONFERENCE: Cisco ATA is connected to two active far ends simultaneously; Cisco ATA performs audio mixing such that every party can hear the other two parties but not themselves.	United States: <ul style="list-style-type: none"> • R—Disconnect the last callee and stay connected with the first party, and revert to CONNECTED state. Sweden: <ul style="list-style-type: none"> • R4—Transfer one FE to the other, drop out of the call, and go to PREDIAL state.
PREDIAL_HOLDING: Cisco ATA user places a connected call on-hold and prepares to dial a second number; Cisco ATA plays dial-tone.	United States and Sweden: <ul style="list-style-type: none"> • *,#—Stop dial-tone, go to CONFIG_HOLDING state, and prepare to collect a configuration command. • 0-9—Stop dial-tone, go to DIALING_HOLDING state, and prepare to complete dialing a second phone number. All Regions: <ul style="list-style-type: none"> • Stop dial-tone, retrieve the WFE, and revert to CONNECTED state.
CONFIG_HOLDING: A connected FE is placed on hold, while the Cisco ATA is entering a configuration command.	United States: <ul style="list-style-type: none"> • *67—CLIR for the next call • *82—CLIP for the next call • #90v#—Blind transfer to the number specified in 'v'; disconnect the call and go to PREDIAL state. Sweden: <ul style="list-style-type: none"> • #31# or *31#—CLIR in the next call • *90*v#—Blind transfer to the number specified in 'v'; disconnect the call and go to PREDIAL (non-standard) state. All Regions: <ul style="list-style-type: none"> • R or any unrecognized sequence—Abort configuration, restart dial tone, and go to PREDIAL_HOLDING state. • A complete configuration sequence—Carry out the command, and go to PREDIAL_HOLDING state.
DIALING_HOLDING: Cisco ATA user is entering a second phone number to call while placing a connected call on hold	<ul style="list-style-type: none"> • Collected digits match a dial-plan rule—Call the new number, and go to CALLING_HOLDING state • R—Abort dialing and revert to PREDIAL_HOLDING state.

Table 6-4 Call Command Behavior (continued)

Cisco ATA State and its Definition	Summary of Commands (Input Sequence and Actions)
CALLING_HOLDING: Cisco ATA is waiting for a second far end to respond while placing a connected call on hold	<ul style="list-style-type: none"> • R—Cancel the call and revert to PREDIAL_HOLDING state. • ONH—Cancel the call and transfer the waiting party to the callee, and revert back to PREDIAL state.
WAITHOOK_HOLDING: The AFE hangs-up to disconnect the current call while there is a WFE being put on hold	<ul style="list-style-type: none"> • R—Retrieve the WFE and go to CONNECTED state.
AITHOOK_ALERTING: The AFE hangs up while a waiting call alerts	<ul style="list-style-type: none"> • R—Stop CWT, answer the waiting call, and go to CONNECTED state. • WFE: Cancel the call; stop CWT, go to WAITHOOK state. • ONH—Go to IDLE state (in which Cisco ATA automatically starts ringing the phone, and goes to RINGING state).



Configuring and Debugging Fax Services

The Cisco ATA provides two modes of fax services that are capable of internetworking with Cisco IOS gateways over IP networks. These modes are called *fax pass-through mode* and *fax mode*.

With *fax pass-through mode*, the Cisco ATA encodes fax traffic within the G.711 voice codec and passes it through the Voice Over IP (VoIP) network as though the fax were a voice call. This mode uses the Cisco proprietary *fax upspeed* method.

With *fax mode*, the Cisco ATA presents itself as a device capable of using only G.711 codecs; therefore, no codec renegotiation or switchover is required. This places minimum functionality and configuration requirements on remote gateways. *Fax mode* is recommended for environments in which G.711 fax upspeed is not available for the supporting Cisco gateways.

This section contains the following topics:

- Using Fax Pass-through Mode, page 7-1
- Using FAX Mode, page 7-6
- Debugging the Cisco ATA 186/188 Fax Services, page 7-7



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.

Using Fax Pass-through Mode

Fax pass-through mode allows for maximum codec flexibility because users may set up a voice call using any voice codec, then renegotiate to a G.711 codec for the fax session. To use *fax pass-through mode*, first configure the Cisco ATA and supporting Cisco gateways to support the Cisco-proprietary G.711 fax upspeed method. Then, disable fax relay on the far-end gateway—either for the entire gateway or for the dial peer engaged in the fax call with the Cisco ATA.

The fax upspeed method allows you to use low bit-rate codecs such as G.723 and G.729 for voice calls, and G.711 codecs for fax calls. With a fax call, the Cisco ATA detects a 2100-Hz CED tone or V.21 preamble flag, then informs the remote gateway of its intent to switchover to G.711 via a peer-to-peer message. This type of message, carried as a Named Signaling Event (NSE) within the RTP stream, is used for all fax event signaling. The Cisco ATA can initiate and respond to NSEs and can function as either an originating or terminating gateway.

**Note**

The Cisco ATA can also accept standard-based protocol-level codec switch requests, but cannot send such requests. Therefore, to interoperate with a Cisco gateway, use the Cisco-proprietary codec switch.

This section contains the following topics:

- Configuring the Cisco ATA for Fax Pass-through mode, page 7-2
- Configuring Cisco IOS Gateways to Enable Fax Pass-through, page 7-3

Configuring the Cisco ATA for Fax Pass-through mode

Fax Pass-through mode requires configuring two configuration parameters:

AudioMode, page 7-2

ConnectMode, page 7-3

AudioMode

Description

The AudioMode parameter is a 32-bit value. The lower 16 bits apply to the **Phone 1** port of the Cisco ATA and the upper 16 bits apply to the **Phone 2** port of the Cisco ATA.

Example

The following is an example of configuring the **Phone 1** port of the Cisco ATA for *fax pass-through mode*:

```
0xFFFF0015
```

Translation

This setting translates to the following bitmap:

```
xxxx xxxx xxxx xxxx 0000 0000 0001 0101
```

- Bit 0 = 1—Enables G.711 silence suppression (VAD)
- Bit 2 = 1—Enables Fax CED tone detection and switchover upon detection
- Bit 4 = 1, Bit 5 = 0—DTMF transmission method = out-of-band through negotiation
- Bit 6 = Bit 7 = 0—Hookflash transmission method = disable sending out hookflash

**Note**

The values xxxx in the example apply to the **Phone 2** port of the Cisco ATA.

To configure the same value for the **Phone 2** port of the Cisco ATA, the value would be 0x0015XXXX. The configuration of one port is independent from the configuration of the other port.

ConnectMode

Description

The ConnectMode parameter is a 32-bit value. The parameter settings apply to both lines of the Cisco ATA. Configure ConnectMode after configuring AudioMode for *fax pass-through mode*. Cisco recommends you use the following ConnectMode setting to interoperate with a Cisco IOS gateway.

Recommended Setting

0x90000400

Translation

This setting translates to the bitmap:

1001 0000 0000 0000 0000 0100 0000 0000

Bit 2 and bits 7 through 15 are the only relevant bits for *fax pass-through mode*. These bits from the example are isolated below:

xxxx xxxx xxxx xxxx 0000 0100 0xxx x0xx

- Bit 2 = 0—Uses RTP payload number 126/127 for fax upspeed to G.711μ-law/G.711A-law. Set this value to 1 if you want to use RTP payload number 0/8 for fax upspeed.
- Bit 7 = 0—Disables fax pass-through redundancy. Set this bit to 1 to enable redundancy. With redundancy enabled, the Cisco ATA sends each packet twice. Because of bandwidth and transmission time costs, use this option only if network quality is poor and all other gateways used in the network support this feature.
- Bits { 12, 11, 10, 9, 8 } = { 0, 0, 1, 0, 0 }—Sets the offset to NSE payload-type number 96 to 4. Setting the offset to 4 results in the Cisco ATA sending an NSE payload-type value of 100 by default. Valid offset values range from 2 to 23 (NSE payload type value of 98 to 119). Set this value to match the value for your Cisco gateways.

Most Cisco MGCP-based gateways, such as Cisco 6608, use NSE payload type 101 by default. Most Cisco H.323/SIP-based gateways use NSE payload type 100 by default.

- Bit 13 = 0—Uses G.711μ-law for fax pass-through upspeed. Set this bit to 1 to use G.711A for fax pass-through upspeed.
- Bit 14 = Bit 15 = 0—Enables *fax pass-through mode* using the Cisco proprietary method (recommended). Set both of these bits to 1 to disable *fax pass-through mode*.

Configuring Cisco IOS Gateways to Enable Fax Pass-through

To configure your IOS gateways to network with Cisco ATA, do the following:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Enable Fax Pass-through Mode, page 7-4 |
| Step 2 | Disable Fax Relay Feature, page 7-5 |
-

**Note**

For detailed information on setting up your IOS gateways and on feature availability, refer to the document *Cisco Fax Services over IP*.

Enable Fax Pass-through Mode

The supporting Cisco gateway can enable *fax pass-through mode* using system-level or dial-peer-level commands.

System Level commands

Enable the fax pass-through feature using the following system-level commands:

Procedure

Step 1 Run the following command:

voice service voip

Step 2 Run the following command:

modem passthrough NSE [payload-type *number*] codec {g711µ-law | g711alaw} [redundancy] [maximum-sessions *value*]

The definitions of the command parameters are as follows:

- The **payload-type** parameter default is 100. Valid values are from 98 to 119.
The NSE payload number must be the same on both the Cisco ATA and the Cisco gateway.
- The **codec** parameter must be G.711µ-law for faxes sent over a T1 trunk or G.711A-law for faxes sent over an E1 trunk.
- The **redundancy** parameter enables RFC 2198 packet redundancy. It is disabled by default.
- The **maximum sessions** parameter defines the number of simultaneous fax pass-through calls with redundancy. The default is 16. Valid values are 1 to 26.

When using the **voice service voip** and **modem passthrough nse** commands on a terminating gateway to globally set up fax or modem pass-through with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number .
```

Step 3 For the Cisco ATA ConnectMode parameter, turn off bits 14 and 15. This enables the sending of fax pass-through signals and the detection of incoming fax pass-through signals using the Cisco proprietary method.

**Note**

The NSE payload-type number, fax pass-through codec (G.711µ-law or G.711A-law) and redundancy parameters must have the same settings for the Cisco ATA that they have for supporting Cisco gateways.

Dial-Peer Level Commands

You can enable *fax pass-through mode* for communication between a Cisco IOS gateway and the specified Cisco ATA using the following dial-peer level commands:

Procedure

-
- Step 1** Perform the command:
- dial-peer voice *tag* voip**
- Step 2** Perform the command:
- modem passthrough {NSE [payload-type *number*] codec {g711µlaw | g711alaw} [redundancy] | system}**
- a. The default of this command is:
- modem passthrough system**
- When using the default configuration, the dial-peer fax pass-through configuration is defined by the **voice service voip** command. When the **system** option is used, no other parameters are available.
- When the NSE is configured in the fax pass-through command at the dial-peer level, the fax pass-through definition in the **dial-peer** command takes priority over the definition in the **voice service voip** command.
- b. The **payload-type *number***, **codec**, and **redundancy** parameters can also be used.
- For example, the command:
- modem passthrough NSE codec g711µlaw**
- means that the Cisco ATA will use the NSE payload-type number 100, G.711µ-law codec, and no redundancy in *fax pass-through mode*.
- Step 3** When setting up dial-peer for fax pass-through, it is necessary to set up a pair of dial-peers for inbound and outbound calls between the Cisco ATA and Cisco IOS gateways. You do this by specifying the **destination-pattern** and **incoming-called number**. The **destination-pattern** should point to the Cisco ATA, while the incoming-called number should apply to all numbers that the Cisco ATA is allowed to dial.
-

Disable Fax Relay Feature

Fax relay may be enabled by default for some IOS gateways. If you do not disable the fax relay feature, it may override the precedence of fax/modem pass-through and cause the fax transmission to fail. It is necessary to disable fax relay at the dial-peer or system level with the following command:

fax rate disable

Using FAX Mode

Use *fax mode* when the gateways in the network do not support *fax pass-through mode* or dial-peer configuration.

You can set one or both lines of the Cisco ATA to G.711-only *fax mode*. This mode allows the fax machine connected to the Cisco ATA to communicate directly with the far endpoint with no fax signaling event occurring between the two gateways.

This section contains the following topics:

- Configuring the Cisco ATA for Fax Mode, page 7-6
- Configuring the Cisco ATA for Fax Mode on a Per-Call Basis, page 7-7
- Configuring the Cisco IOS Gateway for Fax Mode, page 7-7

Configuring the Cisco ATA for Fax Mode

G.711-only *fax mode* operation requires configuration of one parameter—**AudioMode**.

Description

The AudioMode parameter is a 32-bit value. The lower 16 bits apply to the **Phone 1** port of the Cisco ATA, and the upper 16 bits to the **Phone 2** port. The following is an example of the **Phone 1** port of the Cisco ATA configured for G.711-only *fax mode*:

Example

```
0xFFFF0012
```

Translation

This setting translates to the bitmap:

```
xxxx xxxx xxxx xxxx 0000 0000 0001 0010
```

- Bit 0 = 0—Disables G.711 silence suppression (VAD).
- Bit 1 = 1—Uses G.711 only, does not user the low bit-rate codec.
- Bit 2 = 0—Disables Fax CED tone detection.
- Bit 4 = 1, Bit 5 = 0—DTMF transmission method: out-of-band through negotiation
- Bit 6 = Bit 7 = 0—Hookflash transmission method: disables sending out hookflash



Note

The values xxxx in the example do not apply to the **Phone 1** port of the Cisco ATA.

To configure the same value for the **Phone 2** port of the Cisco ATA, the value would be 0x0012xxxx. The configuration of one port is independent from the configuration of the other port.



Note

The AudioMode configuration overrides the values of the following three parameters: RxCodec, TxCodec, and LBRCodec. For example, if these three parameters are each set to 0 (for G.723), the Cisco ATA would still use G.711 if AudioMode is set to 0x00120012. With this configuration, the Cisco ATA sends both G.711μ-law and G.711A-law as preferred codecs to a peer voice gateway.

Configuring the Cisco ATA for Fax Mode on a Per-Call Basis

**Note**

The per-call-basis *fax mode* feature is only available for the H.323 and SIP protocols.

If you want to activate *fax mode* on a per-call basis, configure the following parameters:

Procedure

-
- | | |
|---------------|---|
| Step 1 | CallFeatures and PaidFeatures Bit 15 (for line1—mask 0x8000) and Bit 31 (for line2—mask 0x80000000) = 1: This sets the default to enable <i>fax mode</i> on a per-call basis. |
| Step 2 | AudioMode Bit 2 = 0: This disables fax CED tone detection. |
| Step 3 | CallCmd includes *99;xA (99 is the default; the value can be changed to any prefix code.) |
-

To activate a call from your fax machine, enter ***99** (default), then enter the telephone number to which you want to send the fax. The next call will automatically revert to normal mode.

Configuring the Cisco IOS Gateway for Fax Mode

On the Cisco gateway, disable both fax relay and fax pass-through at the dial-peer level or system level with the following commands:

Procedure

-
- | | |
|---------------|---|
| Step 1 | Run the command:

fax rate disable |
| Step 2 | Run the command:

no modem passthrough |
-

Debugging the Cisco ATA 186/188 Fax Services

This section includes the following debugging topics for fax services:

- Common Problems When Using IOS Gateways, page 7-7
- Using prserv for Diagnosing Fax Problems, page 7-9
- Using rtpcatch for Diagnosing Fax Problems, page 7-12

Common Problems When Using IOS Gateways

Table 7-1 lists typical problems and actions that might solve these problems for situations in which the Cisco ATA is using fax over a Cisco IOS gateway.

Table 7-1 Solving Common Fax Problems

Problem	Action
The far-end gateway is not loaded with correct software image.	Cisco recommends IOS version 12.2 (11)T or higher for the Cisco 2600 and Cisco 3600, and IOS version 12.1 (3)T or higher for Cisco AS5300. The Cisco 6608 supports both the NSE and NTE methods of <i>fax pass-through mode</i> , beginning with software version D004030145S16608. To use <i>fax pass-through mode</i> with the Cisco 6608, the user must select 6608 NSE mode, and the NSE payload type must be reconfigured to match the Cisco ATA.
The Cisco ATA is not loaded with the proper software.	Cisco recommends using software version 2.14 or higher.
User is operating Cisco ATA software on an outdated model.	Cisco recommends using Cisco ATA models 186-I1, 186-I2, 188-I1, or 188-I2 (hardware platforms).
The Cisco ATA is not configured for <i>fax mode</i> or <i>fax pass-through mode</i> .	For <i>fax mode</i> , the AudioMode configuration parameter should be set to 0XXXXX0012 (X = value not applicable) for the Phone 1 port of the Cisco ATA, and 0x0012XXXX for the Phone 2 port. For <i>fax pass-through mode</i> , AudioMode should be set to 0XXXXX0015 for the Phone 1 port of the Cisco ATA, and 0x0015XXXX for the Phone 2 port.
The remote gateway is not configured for modem/ <i>fax pass-through mode</i> .	When the Cisco ATA is configured for <i>fax pass-through mode</i> , all remote gateways must be configured with modem/ <i>fax pass-through mode</i> either on a dial-peer level or system level.
Fax relay is not disabled on the remote gateway.	Fax relay is enabled by default on some Cisco gateways. When fax relay is enabled, it can override <i>fax pass-through mode</i> and cause fax failure. Examples of the CLI commands to disable fax relay for IOS gateways are as follows: <ul style="list-style-type: none"> • fax rate disable for H.323/SIP gateways • mgcp fax t38 inhibit for MGCP gateways
Fax/modem pass-through method on the remote gateway is not compatible with the Cisco NSE-based method.	Some Cisco gateways (such as Cisco VG248, and Cisco 6608) may use signaling messages based on RFC2833 for G.711 upspeed when loaded with older software images. This method is incompatible with the Cisco NSE-based method. You must check to make sure that the image on your gateway supports the Cisco NSE-based fax/modem pass-through. Otherwise, you must configure the Cisco ATA to use <i>fax mode</i> .
NSE payload types differ between gateways.	The Cisco ATA has a configurable NSE packet payload-type value whose default is 100. This value is compatible with the implementations of most Cisco gateways. However, some Cisco gateways use 101 as the NSE payload type. Ensure that all gateways in your environment use the same NSE payload type if you wish to successfully use <i>fax pass-through mode</i> .

Using prserv for Diagnosing Fax Problems

This section contains the following topics:

- prserv Overview, page 7-9
- Analyzing prserv Output for Fax Sessions, page 7-9

prserv Overview

prserv is a tool that runs on a Microsoft Windows-based PC and serves as a log server that captures debug information that the Cisco ATA sends to your PC IP address/port. The debug information is saved into a readable text file.

To enable your Cisco ATA to send debug information, you need to set the **NPrintf** configuration parameter to your PC IP address and an available port, as shown in the following procedure:

Procedure

- Step 1** `<IP address>.<port>`
 `<IP address>` is the IP address of your PC.
 `<port>` is any unused port (any number from 1024 to 65535) on your PC.



Note You can the Nprintf parameter on the Cisco ATA configuration web page or with the TFTP-based configuration method.

- Step 2** To operate the debug capture program prserv.exe, place the prserv program in a folder on your PC. At the DOS prompt, enter:
 `C:>prserv <port>`
 `<port>` is the port number you have selected. If `<port>` is omitted, the default port number is 9001.

As prserv receives debug information from the Cisco ATA, it displays the information on the DOS screen and saves it to the output file `<port>.log`.

Once you are finished capturing debug information, you can stop prserv by entering Ctrl-C at the DOS prompt. If you restart the process without changing the name of the log file, any new debug information is appended to the end of the original file.

Analyzing prserv Output for Fax Sessions

The debug log obtained from **prserv** is for detecting simple configuration problems.



Note

A comprehensive understanding of the fax events requires the use of the **rtptcatch** tool (see the “Using rtptcatch for Diagnosing Fax Problems” section on page 7-12).

Table 7-2 lists log events relevant to analyzing a fax session.

Table 7-2 Debug Log Examples

Log event	Description
[<i>ch</i>] Enable encoder < <i>pt</i> >	Voice encoder type <i>pt</i> is enabled for the channel <i>ch</i> , where <i>pt</i> can be 0 for G.711 μ -law, 4 for G.723.1, 8 for G.711A-law, and 18 for G.729. For example, [0]Enable encoder 4 indicates that the Cisco ATA transmitted G.723.1-encoded voice packets.
[<i>ch</i>] DPKT 1st: < <i>timestamp1</i> > < <i>timestamp2</i> >, pt < <i>pt</i> >	The first voice packet that the Cisco ATA received was of RTP payload type <i>pt</i> for the channel <i>ch</i> with timestamp of <i>timestamp1</i> , and the local decoding timestamp was set to <i>timestamp2</i> . For example, [0]DPKT 1st: 1491513359 1491512639, pt 4 indicates that the first RTP packet that the Cisco ATA received was G.723.1-encoded for channel 0.
[<i>ch</i>] codec: < <i>pt1</i> > => < <i>pt2</i> >	Voice codec switchover occurred. The voice encoder type switched from <i>pt1</i> to <i>pt2</i> for the channel <i>ch</i> . For example, [0]codec: 4 => 0 indicates that the local voice encoder on the Cisco ATA switched from G.723.1 to G.711 μ -law.
[<i>ch</i>] Rx MPT PT=< <i>NSEpt</i> > NSE pkt < <i>event</i> >	Channel <i>ch</i> received an NSE packet of <i>event</i> with payload type of <i>NSEpt</i> . For <i>event</i> , c0XXXXXX indicates a CED tone event, and c1XXXXXX indicates a phase reversal event. For example, [0]Rx MPT PT=100 NSE pkt c0000000 indicates that the Cisco ATA received a CED tone event NSE packet with payload type of 100.
[<i>ch</i>] Tx MPT PT=< <i>pt</i> > NSE pkt < <i>event</i> >	Channel <i>ch</i> transmitted an NSE packet of <i>event</i> with payload type of <i>NSEpt</i> . For <i>event</i> , c0XXXXXX indicates a CED tone event, and c1XXXXXX indicates a phase reversal event. For example, [0]Tx MPT PT=100 NSE pkt c0000000 indicates that the ATA transmitted a CED tone event NSE packet with payload type of 100.

Debugging FAX Pass-through Mode

When the Cisco ATA is configured to use *fax pass-through mode*, the fax call session can be established with an arbitrary voice codec. Once the voice call has been established, fax machines can signal their presence by means of a CED tone or V.21 preamble flag, after which the gateways send NSE packets to initiate switchover.



Note

For *fax pass-through mode*, check the Cisco ATA debug log to verify that it is acting as an originating gateway as well as a terminating gateway.

Terminating-Gateway Example

When the Cisco ATA is used as a terminating gateway for a fax session, make sure the following conditions are true:

- The Cisco ATA transmits CED-tone-event NSE packets.
- The encoder switchover to G.711 occurs during the NSE-packet transaction.

An example debug log for a terminating gateway scenario is show below:

```
[0]Tx MPT PT=100 NSE pkt c0000000
[0]codec: 4 => 0
[0]Rx MPT PT=100 NSE pkt c0000000
```


Note

The NSE response to the CED tone event is not mandatory; some gateways may not send back an NSE response.

Originating-Gateway Example

When the Cisco ATA is used as an originating gateway for a fax session, make sure that the following conditions are true:

- The Cisco ATA receives and responds to CED-tone-event NSE packets.
- The NSE payload type is the same for the received and transmitted NSE packets.
- The encoder switchover to G.711 occurs during NSE-packet transaction.

An example debug log for an originating gateway scenario is shown below:

```
[0]Rx MPT PT=100 NSE pkt c0000000
[0]Tx MPT PT=100 NSE pkt c0000000
[0]codec: 4 => 0
[0]Rx MPT PT=100 NSE pkt c0000000
[0]Rx MPT PT=100 NSE pkt c0000000
```


Note

If your gateway is using a legacy IOS software image, it may not send NSE packets but instead may rely on a straightforward codec switchover mechanism. In this case, a codec switchover event occurs rather than an NSE packet transaction.

Possible Reasons for Failure

If your Cisco ATA does not receive CED-tone-event NSE packets and codec switchover does not occur, the failure may be due to the following reasons:

- The terminating gateway is not configured with fax/modem pass-through.
- The *fax pass-through mode* used by the terminating gateway may not be compatible with the Cisco NSE method.

If the log shows proper NSE packet transaction and G.711 upspeed for your fax session but the session still fails, check that the following conditions are true:

- The Cisco ATA software image version is 2.14 or above.
- The Cisco ATA model number is ATA186-I1, ATA186-I2, ATA188-I1, or ATA188-I2.
- The fax relay option for the remote gateways has been disabled.

Debugging FAX Mode

When the Cisco ATA is configured with *fax mode*, only G.711 codecs are used. You must confirm that only 0 (for G.711 μ -law) or 8 (for G.711A-law) appear in the `Enable encoder` and `DPKT 1st` debug lines. The following example of a debug log shows that G.711 μ -law is used:

```
[0]Enable encoder 0
[0]DPKT 1st: 1491513359 1491512639, pt 0
```

If the numeric codes for the G.711 codecs do not appear in the log, you need to check your **AudioMode** parameter setting on the Cisco ATA.

If the correct G.711 codecs appear in the log but your fax sessions still fail, check that the following conditions are true:

- The Cisco ATA software image version is 2.14 or above.
- The Cisco ATA model number is ATA186-I1, ATA186-I2, ATA 188-I1, or ATA188-I2.
- The fax relay option for the remote gateways has been disabled.

Using rtpcatch for Diagnosing Fax Problems

This section contains the following topics:

- rtpcatch Overview, page 7-12
- Example of rtpcatch, page 7-13
- Analyzing rtpcatch Output for Fax Sessions, page 7-16
- Using rtpcatch to Analyze Common Causes of Failure, page 7-17
- rtpcatch Limitations, page 7-19

rtpcatch Overview

rtpcatch is a tool that provides comprehensive information for a VoIP connection. The tool runs on a Microsoft Windows-based PC and is capable of parsing an output capture file from Network Associates (NAI) Sniffer Pro and identifies significant fax pass-through and fax relay events.

Major functions

rtpcatch includes the following major functions:

- Reads session data from Sniffer Pro capture files.
- Analyzes media streams.
- Stores media streams to files.
- Reports RTP statistics such as the number of RTP packets, the number of RTP frames, the number of lost packets, the number of filler packets during silence suppression periods, and the number of erased packets.

How to Use

To use **rtpcatch**, follow these steps:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Create a working directory for rtpcatch and place the executable file rtpcatch.exe in this directory. |
| Step 2 | Copy your Network Associates Sniffer Pro capture files into this directory. |
| Step 3 | At the DOS prompt of this directory, enter the following command:

: rtpcatch <cap_file> [<prefix>] [options] |

- **<cap_file>** is the NAI Sniffer capture file.
- **<prefix>** is the prefix prepended to the output filenames.

Output Files

The output files of **rtptcatch** include a summary file and audio stream files.

The summary file is **<prefix>.sum** if **<prefix>** is specified, otherwise it is **file.sum**.

Stream files are labeled with an integer tag beginning with 00. Stream files are also tagged with the extension **pcm** for G.711A/G.711μ-law, **723** for G723.1, **729** for G729, **t38** for T.38, and **cfr** for Cisco Fax Relay.

Options

rtptcatch options include:

- **-fax**—to output the fax events for a connection.

The output includes "FAX summary 1" as the interleaved event list for all directions, and "FAX summary 2" as the event list for each direction. The reported events include voice codec change, NSE signalling, and fax relay events.

- **-port <port0> <port1>**—to discard any packets sent from/to this port.

If the NAI Sniffer capture file includes Cisco ATA **prserv** packets, these packets can interfere with **rtptcatch** analysis. Some **prserv** packets might be interpreted as NTE or NSE events. To prevent such interference, you can either disable debugging output on the Cisco ATA (do this by setting the **Nprintf** configuration parameter to 0), configure your NAI Sniffer to filter out the **prserv** packets, or run **rtptcatch** with the **-port** options.



Note

rtptcatch works best for analyzing a single VoIP session. Command-line options can be entered in any order.

Example of rtptcatch

The section contains an example of using **rtptcatch** and includes an explanation of its output:

Output

```
C:\>rtptcatch faxpassthru -fax

[ 25]open file: 00.723, (G723) 2.213:10000 => 2.116:10002
[ 26]open file: 01.723, (G723) 2.116:10002 => 2.213:10000
[ 29] <00> 1 silence pkts from TS 1760 (seq# 3)
[ 42] <00> 2 silence pkts from TS 4400 (seq# 9)
[ 47] <00> 2 silence pkts from TS 5600 (seq# 11)
[ 55] <00> 2 silence pkts from TS 7760 (seq# 15)
[101]open file: 02.pcm, (G711u) 2.116:10002 => 2.213:10000
[106] <02> 2 lost pkts from seq# 39
[107]open file: 03.pcm, (G711u) 2.213:10000 => 2.116:10002
[110] <03> 1 silence pkts from TS 19440 (seq# 41)
```

----- Summary -----

```

Input file: faxpassthru.cap

<00.723>: (G723) 2.213:10000 => 2.116:10002
        total 38 pkts(70 frames), lost 0 pkts, fill 7 silence pkts

<01.723>: (G723) 2.116:10002 => 2.213:10000
        total 38 pkts(76 frames), lost 0 pkts, fill 0 silence pkts

<02.pcm>: (G711u) 2.116:10002 => 2.213:10000
        total 2181 pkts(2181 frames), lost 2 pkts, fill 0 silence pkts

<03.pcm>: (G711u) 2.213:10000 => 2.116:10002
        total 2179 pkts(2179 frames), lost 0 pkts, fill 1 silence pkts

----- FAX Summary 1 -----

[ 25]<2.213=>2.116> Codec G723
[ 26]<2.116=>2.213> Codec G723
[ 101]<2.116=>2.213> Codec G711u/D
[ 102]<2.116=>2.213> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 103]<2.116=>2.213> NSE PT 100, EVT 193: ECAN OFF, Phase Reversal Detected
[ 105]<2.213=>2.116> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 107]<2.213=>2.116> Codec G711u/D

----- FAX Summary 2 -----

PATH: 2.213:10000 => 2.116:10002
[ 25]Codec G723
[ 105]NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 107]Codec G711u/D

PATH: 2.116:10002 => 2.213:10000
[ 26]Codec G723
[ 101]Codec G711u/D
[ 102]NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 103]NSE PT 100, EVT 193: ECAN OFF, Phase Reversal Detected

```

Explanation

The output is printed on screen and saved in the file file.sum.

The following lines are described:

- [25]open file: 00.723, (G723) 2.213:10000 => 2.116:10002
This indicates that **rtpcatch** reached NAI Sniffer packet number 25 and opened a new file named 00.723 to store an audio stream consisting of G.723-compressed data. The audio path originates from the IP address ending with 2.213 and port 10000 (written as <2.213:1000>) and terminates at the IP address ending with 2.116 and port 10002.
- [29] <00> 1 silence pkts from TS 1760 (seq# 3)
This indicates that **rtpcatch** detected one silence RTP packet in the audio path <00> and the silence packet began at timestamp 1760. This occurred at packet number 29 with the RTP sequence number 3.
- [106] <02> 2 lost pkts from seq# 39
This indicates that **rtpcatch** detected two lost RTP packets in the audio path <02>. The missing packets began with sequence number 39. This occurred at packet number 106.

- ----- Summary -----

```
Input file: faxpassthru.cap
<00.723>: (G723) 2.213:10000 => 2.116:10002
total 38 pkts(70 frames), lost 0 pkts, fill 7 silence pkts
```

This indicates that the input filename is faxpassthru.cap. The output file 00.723 contains the G.723-compressed stream from <2.123:10000> to <2.116:10002>; 38 packets (70 frames) were processed by **rtptcatch**. No lost packets were detected and seven silence packets were found.

- ----- FAX Summary 1 -----

```
[ 25]<2.213=>2.116> Codec G723
[ 26]<2.116=>2.213> Codec G723
[ 101]<2.116=>2.213> Codec G711u/D
[ 102]<2.116=>2.213> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 103]<2.116=>2.213> NSE PT 100, EVT 193: ECAN OFF, Phase Reversal Detected
[ 105]<2.213=>2.116> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 107]<2.213=>2.116> Codec G711u/D
```

This indicates that the audio streams originating at <2.213> and <2.216> are G.723-compressed. The audio stream from <2.116> was then up-spiced to G.711 μ -law at packet number 101. The NSE signaling packets were sent at packet number 102, 103 and 105. Finally, the audio stream from <2.113> was up-spiced to G.711 μ -law.

- ----- FAX Summary 2 -----

```
PATH: 2.213:10000 => 2.116:10002
[ 25]Codec G723
[ 105]NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 107]Codec G711u/D

PATH: 2.116:10002 => 2.213:10000
[ 26]Codec G723
[ 101]Codec G711u/D
[ 102]NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 103]NSE PT 100, EVT 193: ECAN OFF, Phase Reversal Detected
```

This summarizes the fax events for each path.

The audio stream events reported by **rtptcatch** include:

- beginning of new audio codec
- silence packets
- lost packets
- erased packets (as in G.729)

The NSE events reported by **rtptcatch** include:

- event 32, Fax Mode, CED tone Detected (RFC2833)
- event 34, Modem Mode, ANSam tone Detected (RFC2833)
- event 192, Up-Speed, CED tone Detected
- event 193, ECAN OFF, Phase Reversal Detected
- event 194, ECAN ON, Silence Detected
- event 200, T38 Fax Mode, V.21 Detected
- event 201, T38 Fax Mode ACK
- event 202, T38 Fax Mode NACK

- event 203, Modem Relay Mode, CM Tone Detected
- event Cisco Fax Relay (with RTP payload type 96)
- event Cisco Fax Relay ACK (with RTP payload type 97)

Analyzing rtpcatch Output for Fax Sessions

The following examples show the proper fax events when gateways are configured to operate in the following modes:

- Cisco ATA *fax mode*
- Cisco ATA *fax pass-through mode*
- T.38 fax relay mode
- Cisco fax relay mode

Example 7-1 Fax Mode

```
----- FAX Summary 1 -----
[ 25]<2.131=>3.200> Codec G711u
[ 26]<3.200=>2.131> Codec G711u
```

Analysis

Both sides use G.711 for the entire fax session.

Example 7-2 Fax Pass-through Mode

```
----- FAX Summary 1 -----
[ 25]<2.213=>2.116> Codec G723
[ 26]<2.116=>2.213> Codec G723
[ 101]<2.116=>2.213> Codec G711u/D
[ 102]<2.116=>2.213> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 103]<2.116=>2.213> NSE PT 100, EVT 193: ECAN OFF, Phase Reversal Detected
[ 105]<2.213=>2.116> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 107]<2.213=>2.116> Codec G711u/D
```

Analysis

- Both sides initially use G.723.
- <2.116> switches to G.711 μ -law using a dynamic payload type.
- NSE signaling packets are sent from <2.116>.
- An optional NE signaling packet is sent from <2.213>.
- <2.113> switches to G.711 μ -law using a dynamic payload type.



Note

EVT 193 may not appear for some fax transmission.

Example 7-3 Fax Pass-through Mode

```
----- FAX Summary 1 -----
[ 37]<3.200=>2.53> Codec G723
[ 41]<2.53=>3.200> Codec G723
```

```
[ 136]<3.200=>2.53> Codec G711u/D
[ 137]<3.200=>2.53> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 140]<2.53=>3.200> Codec G711u/D
```

Analysis

- Both sides initially use G.723.
- <3.200> switches to G.711 μ -law using a dynamic payload type.
- NSE signaling packets are sent from <3.200>.
- <2.53> switches to G.711 μ -law using a dynamic payload type.

Example 7-4 T38 Fax Relay Mode

```
----- FAX Summary 1 -----
[ 15]<2.53=>3.99> Codec G711u
[ 486]<3.99=>2.53> Codec G711u
[ 1277]<3.99=>2.53> Codec T38
[ 1278]<2.53=>3.99> Codec T38
```

Analysis

- Both sides initially use G.711 μ -law.
- Both sides switch to T.38

Example 7-5 Cisco Fax Relay

```
----- FAX Summary 1 -----
[ 8]<2.53=>3.99> Codec G711u
[ 248]<3.99=>2.53> Codec G711u
[ 798]<2.53=>3.99> NSE PT 96, Cisco Fax Relay
[ 799]<3.99=>2.53> NSE PT 97, EVT 192: Up-Speed, CED tone Detected
[ 800]<2.53=>3.99> NSE PT 97, Cisco Fax Relay ACK
[ 801]<2.53=>3.99> Codec C_FxRly
[ 803]<3.99=>2.53> NSE PT 96, EVT 192: Up-Speed, CED tone Detected
[ 804]<2.53=>3.99> NSE PT 97, Cisco Fax Relay ACK
[ 805]<3.99=>2.53> Codec C_FxRly
```

Analysis

- Both sides initially use G.711 μ -law.
- NSE signaling packets are sent between <2.53> and <3.99>.
- Both sides switch to Cisco fax relay.

Using rtpcatch to Analyze Common Causes of Failure

The following examples show the **rtpcatch** output of failed fax sessions. <3.200> is ATA; <2.53> is a Cisco gateway.

Example 7-6 Cisco ATA Configuration Failure

```
----- FAX Summary 1 -----
```

```
[ 37]<2.53=>3.200> Codec G723
[ 39]<3.200=>2.53> Codec G723
```

Analysis

- <2.53> is the originating gateway and <3.200> is the terminating Cisco ATA.
- The Cisco ATA and the <2.53> gateway use G.723 codec.

Possible Causes for Failure

- The Cisco ATA is not configured with *fax mode* or *fax pass-through mode*.
- If the Cisco ATA is the gateway for a fax sender, the remote gateway is not configured with *fax pass-through mode*.

Example 7-7 Fax Mode Failure

```
----- FAX Summary 1 -----
[ 37]<2.53=>3.200> Codec G711
[ 39]<3.200=>2.53> Codec G711
[ 1820]<2.53=>3.200> NSE PT 96, Cisco Fax Relay
[ 1966]<2.53=>3.200> NSE PT 96, Cisco Fax Relay
```

Analysis

- <2.53> is the originating gateway and <3.200> is the terminating Cisco ATA.
- The Cisco ATA and the <2.53> gateway begin with G.711 codec.
- The <2.53> gateway sends Cisco fax relay event packets.

Possible Cause for Failure

- Cisco fax relay option is not disabled on the gateway.

Example 7-8 Fax Pass-through Mode Failure

```
----- FAX Summary 1 -----
[ 2]<2.53=>3.200> Codec G723
[ 4]<3.200=>2.53> Codec G723
[ 106]<3.200=>2.53> Codec G711u/D
[ 107]<3.200=>2.53> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 1436]<3.200=>2.53> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
```

Analysis

- <2.53> is the originating gateway, and <3.200> is the terminating Cisco ATA.
- The Cisco ATA upspeeds to G.711 μ -law and sends G.711 upspeed NSE signaling packets.
- The <2.53> gateway does not respond to the NSE signaling packets.

Possible Causes for Failure

- Fax/modem pass-through option is not enabled on the gateway.
- Fax/modem pass-through NSE payload type are configured differently on the Cisco ATA and the gateway.

Example 7-9 Fax Pass-through Mode Failure

```

----- FAX Summary 1 -----
[ 37]<2.53=>3.200> Codec G723
[ 39]<3.200=>2.53> Codec G723
[ 143]<3.200=>2.53> Codec G711u/D
[ 144]<3.200=>2.53> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 1602]<3.200=>2.53> NSE PT 100, EVT 192: Up-Speed, CED tone Detected
[ 1604]<2.53=>3.200> Codec G711u/D
[ 1820]<2.53=>3.200> NSE PT 96, Cisco Fax Relay
[ 1966]<2.53=>3.200> NSE PT 96, Cisco Fax Relay

```

Analysis

- <2.53> is the originating gateway, and <3.200> is the terminating Cisco ATA.
- The Cisco ATA upspeeds to G.711 μ -law and sends G.711 upspeed NSE signaling packets.
- The <2.53> gateway upspeeds to G.711 μ -law and then sends Cisco fax relay event packets.

Possible Cause for Failure

- Cisco fax relay option is not disabled on the gateway.

Example 7-10 Fax Pass-through Mode Failure

```

----- FAX Summary 1 -----
[ 33]<3.200=>2.53> Codec G729
[ 39]<2.53=>3.200> Codec G729
[ 562]<2.53=>3.200> NTE PT 101, EVT 34: Modem Mode, ANSam tone Detected (RFC2833)
[ 563]<2.53=>3.200> NTE PT 101, EVT 34: Modem Mode, ANSam tone Detected (RFC2833)
[ 565]<2.53=>3.200> NTE PT 101, EVT 34: Modem Mode, ANSam tone Detected (RFC2833)
[ 566]<2.53=>3.200> Codec G711u/D
[ 568]<2.53=>3.200> NTE PT 101, EVT 34: Modem Mode, ANSam tone Detected (RFC2833)
[ 580]<3.200=>2.53> Codec G711u/D

```

Analysis

- <3.200> is the originating Cisco ATA, and <2.53> is the terminating gateway.
- Both sides initially use G.729.
- <2.53> gateway sends NTE signaling packets, then upspeeds to G.711 μ -law.
- <3.200>The Cisco ATA switches to G.711 μ -law also, but never sends NTE signaling packets.
- Fax transmission fails because <2.53> gateway does not receive any NTE packets, and it drops the fax call.

Possible Cause for Failure

- The Cisco ATA does not support the NTE signaling method and requires that the gateways use the NSE signaling method.

rtpcatch Limitations

- **rtpcatch** performs optimally when analyzing capture files containing only one VoIP session.
- **rtpcatch** detects only G.711A, G.711 μ -law, G.723, G.729, T.38, Cisco fax relay, modem pass-through with or without redundancy packets, RTCP packets and NSE packets.

- **rtpcatch** can handle a maximum of 20 prserv ports using the -port option.
- **rtpcatch** may not detect T.38 packets correctly.



Upgrading the Cisco ATA Signaling Image

This section describes two methods for upgrading the Cisco ATA software for the SIP protocol:

- Upgrading the Signaling Image from a TFTP Server, page 8-1—This is the Cisco-recommended method for the SIP protocol. This method is the most efficient method and requires only a one-time configuration change.
- Upgrading the Signaling Image Manually, page 8-2—This method can be used if you must manually upgrade the image of one Cisco ATA. However, this method is not the recommended upgrade method because it is not as simple as the TFTP method.

This section also describes procedures for verifying a successful image upgrade:

- Confirming a Successful Signaling Image Upgrade, page 8-5—Procedures for using your Web browser or the voice configuration menu are included.



Caution

Do not unplug the Cisco ATA while the function button is blinking. Doing so can cause permanent damage to the device. The function button blinks during an upgrade.



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.

Upgrading the Signaling Image from a TFTP Server

You can configure the Cisco ATA to automatically download the latest signaling image from the TFTP server. You do this configuring the parameter *upgradecode* in your Cisco ATA configuration file. (You also would use this procedure if you wanted to perform a cross-protocol signaling image upgrade.) For more information about setting up the configuration file, see the “Creating Unique and Common Cisco ATA Configuration Files” section on page 3-8.

Syntax of upgradecode Parameter

```
upgradecode:3,0x301,0x0400,0x0200,tftp_server_ip,69,image_id,image_file_name
```

Definitions

- The hexadecimal values that precede the *tftp_server_ip* variable must always be the values shown in the syntax.
- *tftp_server_ip* is the TFTP server that contains the latest signaling image file.

- `image_id` is a unique 32-bit integer that differs with each upgrade. You can determine this 32-bit integer value by using the build date on the image file name and prepending it with "0x". For example, if the `image_file_name` is `ata186-v2-14-020514a.kxz`, then the build date is 020508a, and the `image_id` is 0x020508a).
- `image_file_name` is the firmware upgrade-image file name. The `image_file_name` format is:
`ata186-v{M}-{N}-{yyymmdd}{a-f}{ext}`
 - `M` is the major version number
 - `N` is the minor version number (always two digits)
 - `yyymmdd` is a two-digit year, two-digit month, and two-digit day
 - `a-f` is the build letter (- `yyymmdd` and `a-f` together form the build date of the image)
 - `ext` must be ".kxz" for upgrading from version 2.11 and below, and can be ".zup" for upgrading from version 2.12 and up for the Cisco ATA186, but it *must* be ".zup" for upgrading the Cisco ATA188.

Process

Whenever the Cisco ATA administrator stores a new signaling image (denoted by a change to the `image_id`), the Cisco ATA upgrades its firmware with the new `image_file`. To contact the TFTP server, the Cisco ATA uses the TFTP server IP address that is contained within the value of the `upgradecode` parameter.

Example

The `upgradecode` parameter value could be:

```
upgradecode:3,0x301,0x0400,0x0200,192.168.2.170,69,0x020723a,ata186-v2-15-020723a.zup
```

This instructs the Cisco ATA to upgrade its firmware to `ata186-v2-15-020723a.zup` by downloading the `ata186-v2-15-020723a.zup` file from the TFTP server IP address of 192.168.2.170. This download occurs after the Cisco ATA downloads its configuration file that contains the directive from the `upgradecode` parameter. Also, the upgrade occurs only if the internally cached `image_id` in Cisco ATA is different from the value 0x020723a.

Upgrading the Signaling Image Manually

This section describes how to manually upgrade the Cisco ATA with the most recent signaling image. The executable file that you need is called `ata186us.exe`, and is bundled in the Cisco ATA release-software zip file.

This section contains the following topics:

- Preliminary Steps, page 8-3
- Running the Executable File, page 8-3

Preliminary Steps

Before you run the executable file, be sure to complete the following procedure:

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** Locate 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 signaling image file (this file has an extension of .zup—For example, ata186-v2-15-020723a.zup) and store it on the PC that has connectivity with the Cisco ATA.
- Step 3** Set the Cisco ATA parameter UseTftp to 0.



Note Remember to set this parameter back to 1 before you use the TFTP upgrade method at a later time.

- Step 4** Follow the instructions in the “Running the Executable File” section on page 8-3.
-

Running the Executable File

This section includes the procedure for running the executable file and using the voice configuration menu to complete the upgrade process. First check to make sure the upgrade requirements are met and determine the syntax to use when running the program.

This section contains the following topics:

- “Upgrade Requirements” section on page 8-3
- “Syntax” section on page 8-3
- “Upgrade Procedure” section on page 8-4

Upgrade Requirements

The following list contains the requirements for using the ata186us.exe file and the voice configuration menu to upgrade the Cisco ATA to the latest signaling image:

- A network connection between the PC from which you will invoke the executable file and the Cisco ATA
- A PC running Microsoft Windows 9X/ME/NT/2000

Syntax

```
ata186us [-any] {-h[host_ip]} {-p[port]} {-quiet} [-d1 -d2 -d3] <image file>
```

Definitions

- -any—Allow upgrade regardless of software and build versions (recommended).
- -h [host_ip]—Set the upgrade server to a specific IP address in cases where there may be more than one IP address for the host. The default behavior is that the program will use the first IP address it obtains when it runs the **gethostbyname** command.
- -p [port]—Set the server port to a specific port number (the default port number is 8000; use a different port number only if you are setting up an upgrade server other than the default).
- -quiet—Quiet mode; send all output to log file named as [port].log (useful when running the upgrade server as a daemon).
- -d1, -d2, -d3—Choose a verbosity level for debugging, with -d3 being the most verbose.
- image file—This is the name of the signaling image file to which the Cisco ATA will upgrade.

Example

To upgrade the Cisco ATA to the signaling image ata186-v2-15-020723a.zup, you can use the following syntax:

```
ata186us -any -d1 ata186-v2-15-020723a.zup
```

Upgrade Procedure

To perform the upgrade, follow these steps:

Procedure

-
- Step 1** Run the executable file (see the “Syntax” section on page 8-3) from the Microsoft Windows DOS or command prompt. You will receive instructions on how to upgrade.
- Step 2** On the Cisco ATA, press the function button to invoke the voice configuration menu.
- Step 3** Using the telephone keypad, enter the following:

```
100# ip_address_of_PC * port #
```

This is the IP address of the PC and the port number at the DOS prompt where you invoked the ata186us.exe file.

For example, if the IP address is 192.168.1.10, and the port number is 8000 (the default), then enter:

```
100#192*168*1*10*8000#
```

When the upgrade is complete, the "Upgrade Successful" prompt will sound.

**Note**

When upgrading many Cisco ATAs manually, you can save the software-upgrade dial-pad sequence in your telephone's speed-dial, and use this sequence repeatedly.

Confirming a Successful Signaling Image Upgrade

You can verify that you have successfully upgraded the Cisco ATA signaling image by using one of the following methods:

- Using a Web Browser, page 8-5
- Using the Voice Configuration Menu, page 8-5

Using a Web Browser

To use your web browser to verify a successful image upgrade, perform the following steps:

Procedure

Step 1 Open your web browser.

Step 2 Enter the IP address of your Cisco ATA Web configuration page:

`http://<IP address>/dev`

Step 3 Refresh the page to clear the cache.

The image version number and its build date should appear at the bottom-left corner of the Cisco ATA Web configuration page.

Using the Voice Configuration Menu

To use the voice configuration menu to verify a successful image upgrade, perform the following steps:

Procedure

Step 1 Pick up the telephone handset attached to the **Phone1** port of the Cisco ATA.

Step 2 Press the function button on the Cisco ATA.

Step 3 Press **123#** on the telephone keypad to play out the image version number.

Step 4 Press **123123#** on the telephone keypad to play out the image build date.



Troubleshooting

This section describes troubleshooting procedures for the Cisco ATA:

- General Troubleshooting Tips, page 9-1
- Symptoms and Actions, page 9-2
- Installation and Upgrade Issues, page 9-3
- Debugging, page 9-4
- Frequently Asked Questions, page 9-5
- Contacting TAC, page 9-6



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.

General Troubleshooting Tips

The suggestions in this section are general troubleshooting tips.

- Make sure that the DHCP server is operating correctly. Note that the function button blinks slowly when the Cisco ATA attempts to acquire the DHCP configuration.
- If the green activity LED is not flashing after you connect the Ethernet cable, make sure that both the power cord and the Ethernet connection are secure.
- If there is no dial tone, make sure that the telephone line cord from the telephone is plugged into the appropriate port on the Cisco ATA. Make sure that your Cisco ATA is properly registered on your Call Control system. Test another phone; if this phone does not work either, there may be a problem with the current configuration or with the Cisco ATA.
- A busy tone indicates that the party you called is not available. Try your call again later. A fast-busy tone indicates that you dialed an invalid number.
- After power up, if the function button continues to blink slowly, the Cisco ATA cannot locate the DHCP server. Check the Ethernet connection and the availability of the DHCP server.
- The DHCP server should show an incoming request from the MAC address listed on the product label or given by the voice prompt.
- If you place a call to another IP telephone, detect ringing, and the called party answers but you cannot detect the speaker's voice, verify that the Cisco ATA and the other IP telephone support at least one common audio codec: G.711A-law, G.711μ-law, G.723.1, or G.729A.

Symptoms and Actions

Symptom Parameters with values set by using the web server interface or voice configuration menu revert to their original settings.

Possible Cause You are using TFTP for configuration (the UseTFTP parameter is set to 1). The Cisco ATA has a cached version of its configuration file stored in its flash memory; this is what displayed or played through the web server interface or voice configuration menu. If UseTFTP is set to 1, then the cached value of the Cisco ATA configuration file is synchronized with its configuration file located at the TFTP server. This synchronization update of the cached value occurs at approximate intervals determined by the CFGInterval parameter value as well as when the Cisco ATA powers up or resets.

Recommended Action If you are using TFTP for configuration, do not use the web server interface or voice configuration menu to modify the value of the Cisco ATA configuration file. Use the web server interface or voice configuration menu only to initially configure the Cisco ATA to contact the TFTP server for the Cisco ATA configuration file.

Symptom Unable to access the web configuration page.

Possible Cause Software versions earlier than 2.0 require the web configuration page to be enabled using option 80# on the voice configuration menu.

Recommended Action Upgrade the software.

Symptom The Cisco ATA does not seem to be configured using the TFTP server.

Possible Cause The TFTP server address is not properly set.

Recommended Action Ensure that the TftpURL is correctly set to the URL or IP address of the TFTP server that is hosting the configuration file for the Cisco ATA. If you are using DHCP to supply the TFTP server IP address, make sure that the TftpURL is set to 0. Also, unless the TftpURL is an IP address, be sure that the DNS1IP and DNS2IP values are properly set to resolve the TftpURL supplied by DHCP.

Symptom The Cisco ATA contacts the TFTP server more often than specified in the CfgInterval parameter.

Possible Cause The ToConfig parameter is not set to 0.

Recommended Action After the Cisco ATA has a valid configuration file, the ToConfig parameter must be set to 0. If it is not set to 0, the Cisco ATA will attempt to contact the TFTP server too frequently.

Symptom Cannot place call.

Possible Cause Equipment failure on the network.

Recommended Action Replace defective network equipment.

Possible Cause Recipient has not registered the IP phone.

Recommended Action Register the IP phone.

Possible Cause Ethernet cable is not connected.

Recommended Action Make sure that all cables are connected.

Symptom Fast busy tone.

Possible Cause Authentication credential is incorrect.

Recommended Action Verify authentication credential, and revise if necessary.

Possible Cause Recipient has not registered the IP phone.

Recommended Action Register the IP phone.

Possible Cause No common codec between the Cisco ATA and remote end.

Recommended Action Change codec to one that is common with the Cisco ATA and the remote end.

Possible Cause Recipient is in a call with call waiting disabled.

Recommended Action Attempt to place the call at a later time.

Installation and Upgrade Issues



Note

The following issues apply to the manual image-upgrade process only. Image upgrades must be performed separately.

Symptom The red LED is flashing slowly on the function button.

Possible Cause The Cisco ATA is trying to obtain the DHCP address or the software image is being upgraded.

Possible Cause The Ethernet cable is unplugged.

Recommended Action Plug in the Ethernet cable.

Symptom Voice prompt returns *Upgrade not available* message. This can only occur if you are using the executable-file upgrade method.

Possible Cause You are attempting to upgrade to the existing version.

Recommended Action You do not need to upgrade.

Symptom Voice prompt returns *Upgrade failed* message. This can only occur if you are using the executable-file upgrade method.

Possible Cause You have entered an incorrect IP address.

Recommended Action Enter the correct IP address.

Possible Cause Software image is corrupted.

Recommended Action Upgrade software image.

Symptom No dial tone.

Possible Cause No user ID was entered.

Recommended Action Enter the correct user ID.

Symptom Incorrect dial tone.

Possible Cause Check the web interface for your DialTone setting. The default is *U.S.*

Recommended Action Set the correct country DialTone value.

Debugging

The MS-DOS Windows-based debugging program tool, *prserv.exe*, is included in every software upgrade package. The tool is also available from Cisco TAC. The *prserv* program is used in conjunction with the *NPrintf* configuration parameter. This file serves as an upgrade server that captures debug information sent by the Cisco ATA software to your PC's IP address and port number. This debug file (*prserv.exe*) compiles the information from the Cisco ATA into a readable log file. To capture this "NPRINTF" information, you must know the IP address of the PC using the *prserv* program, illustrated as follows:

IP address.port

where *IP address* is the IP address of your PC, and *port* is 9001. If another process on your PC already uses port 9001, you may use some other value (legal values are from 1024 to 65535). If no port value is entered, the default value is 9001.

To enter the IP address and port number, use voice menu option 81#. You must enter the IP address and port number in alphanumeric format, which requires entering the * key after every character entered. To enter the "." character, you must enter the sequence 1 1#.

For example, for a computer with the IP address 172.28.78.90 and port number 9001 (172.28.78.90.9001), you would enter the following on your telephone handset:

1* 7* 2* 1 1* 2* 8* 1 1* 7* 8* 1 1* 9* 0* 1 1* 9* 0* 0* 1* *

To operate the debug capture program *prserv.exe*, place the *prserv* program in a folder on your PC; then at the DOS prompt of the folder where you have placed it, enter:

```
C:> prserv port.log
```

where *port* is the port number you have selected. If you do not enter **port.log**, debug information still appears on your screen, but it is not saved to a log file.

After you finish capturing debug information, you can stop the log program by entering Ctrl-C at the DOS prompt. The log file created is named **port.log**. If you restart the process without changing the name of the log file, any new debug information is appended to the end of the original file.

Contact Cisco TAC for more information. See the “Obtaining Technical Assistance” section on page xvi for instructions.

You should also have access to a sniffer or LAN analyzer.



Caution

For security reasons, Cisco recommends that you do not use the web interface over the public network. Disable the web interface, using the UIPassword parameter, before the Cisco ATA is moved from the service provider site.

Frequently Asked Questions

Q. How can I recover the box if I forgot the password?

A. There are two important passwords. One is the UIPassword, which protects access to the Cisco ATA Web Server interface; the other is the EncryptKey, which protects access to the TFTP configuration file. If you forget the value for the UIPassword but still have access to TFTP-stored configuration file, you can modify the UIPassword via TFTP. However, if you are not configuring the Cisco ATA via TFTP, or if you forget both passwords, the only way you can recover the box is to have physical access to the box and do a factory reset on the box via the box voice configuration menu interface (Access Code: FACTRESET#).

Q. What is the maximum distance from which I can drive an analog device with a Cisco ATA?

A. Table 9-1 provides maximum distances for this question.

Table 9-1 Ring Loads and Distances

Ring Load (per RJ-11 FXS Port)	Maximum Distance
5 REN	200 feet (61 m)
4 REN	1000 feet (305 m)
3 REN	1700 feet (518 m)
2 REN	2500 feet (762 m)
1 REN	3200 feet (975 m)

The Cisco ATA, however, is not designed for long distance. The simple test is to determine if the phone or phones that are connected to the Cisco ATA work properly in their environment.

Pay attention to the following questions:

1. Can the Cisco ATA detect on/off hook from the analog phone?
2. Can the Cisco ATA detect the DTMF signal?
3. Can you dial the remote side?
4. Can the Cisco ATA ring the phone?

5. Is voice quality satisfactory?

If you answer no to any of the above questions, you may have a loop impedance greater than 400 ohm. In this case, perform the following procedure.

Procedure

-
- | | |
|---------------|--|
| Step 1 | Increase the wire gauge to reduce the impedance until the Cisco ATA can detect on/off hook and DTMF signal. |
| Step 2 | If the Cisco ATA cannot ring the phone, find a phone that can ring at a lower ringing voltage. Also, try to use only one phone instead of multiple phones in parallel. |
-

Q. Does the Cisco ATA support an overhead paging system, and, if so, does the Cisco ATA support power denial?

A. The Cisco ATA supports an overhead paging system *only* if that system does not require power denial (battery removal) when a call is disconnected. However, the Cisco ATA can be configured to reverse the voltage polarity when a call is connected or disconnected. For more information, see the “Polarity” section on page 5-27.

Contacting TAC

Qualified customers who need to contact the Cisco Technical Assistance Center (TAC) must provide the following information:

- Product codes.
- Software version number—To identify the software revision number, use the configuration menu number **123**.
- Hardware version number—To identify the hardware revision number, use the serial number and MAC address found on the label on the bottom of the Cisco ATA. The MAC address can also be obtained using voice menu option 24.
- Software build information—To identify the software build information, use the voice menu option **123123**.
- Cisco ATA serial number.

See the “Obtaining Technical Assistance” section on page xvi for instructions on contacting TAC.



Note

Customers who obtained their equipment through service providers, independent dealers and other third parties must contact their equipment provider for technical assistance.



Using SIP Supplementary Services

SIP supplementary services are services that you can use to enhance your telephone service. These services include call forward, call return, call forwarding and conference calling. Use the following parameters to enable and subscribe to supplementary services:

- CallFeatures, page 5-23—Use this parameter to enable desired features.
- PaidFeatures, page 5-24—Use this parameter to subscribe or unsubscribe to enabled features.
- This section contains the following topics:
 - Changing Call Commands, page A-1
 - Cancelling a Supplementary Service, page A-1
 - Common Supplementary Services, page A-1

Changing Call Commands

To change the command for a supplementary service (for example, to change ***69** to ***100**), change the context identifiers in the Call Command field on the Web configuration page. For more information, see Chapter 6, “Call Commands.”



Note

You cannot change supplementary services by means of the voice configuration menu.

Cancelling a Supplementary Service

You can deactivate some supplementary services by pressing ***70** before making a call. You can also configure your system to have services disabled by default and enabled on a call-by-call basis. Use the 32-bit Call Features plan to handle your services in this manner. For more information, see the “CallFeatures” section on page 5-23.

Common Supplementary Services

The supplementary services described in this section, and their configuration and implementation, depend on the system of the country in which the service is activated. For information about your country’s implementation of services, contact your local Cisco equipment provider.

This section contains the following topics:

- Caller ID, page A-2
- Call-Waiting Caller ID, page A-2
- Voice Mail Indication, page A-2
- Unattended Transfer, page A-3
- Attended Transfer, page A-4
- Making a Conference Call in the United States, page A-4
- Making a Conference Call in Sweden, page A-4
- Call Waiting in the United States, page A-5
- Call Waiting in Sweden, page A-5
- About Call Forwarding, page A-5
- Call Forwarding in the United States, page A-5
- Call Forwarding in Sweden, page A-6
- Call Return in the United States, page A-6
- Call Return in Sweden, page A-6
- Calling Line Identification Presentation, page A-6
- About Calling Line Identification Restriction, page A-6
- Calling Line Identification Restriction in the United States, page A-7
- Calling Line Identification Restriction in Sweden, page A-7

Caller ID

When the telephone rings, the Cisco ATA sends a Caller ID signal to the telephone between the first and second ring (with name, telephone number, time, and date information, if these are available).

Call-Waiting Caller ID

The Cisco ATA plays a call waiting tone, then sends an off-hook Caller ID signal to the telephone immediately after the first tone burst.

The Cisco ATA sends the name, telephone number, time, and date information, if these are available.

Voice Mail Indication

This feature allows the Cisco ATA to play an intermittent dial tone if there is a message in the user's voice mail box.

Unattended Transfer

This feature allows a user to transfer an existing call to another telephone number without waiting for the dialed party to answer before the user hangs up. Two methods exist for performing an unattended transfer:

- Semi-unattended Transfer, page A-3
- Fully Unattended Transfer, page A-3

Semi-unattended Transfer

Perform the following steps to complete a semi-unattended transfer:

Procedure

-
- | | |
|---------------|---|
| Step 1 | Press the flash button on the telephone handset to put the other party on hold and get a dial tone. |
| Step 2 | Dial the telephone number to which you would like to transfer the other party. |
| Step 3 | Wait for at least one ring and then hang up your phone to transfer the other party. |
-

Fully Unattended Transfer

Perform the following steps to complete a fully unattended transfer:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Press the flash button on the telephone handset to put the other party on hold and get a dial tone. |
| Step 2 | Press #90 (the transfer service activation code) on your telephone keypad, then enter the phone number to which you want to transfer the other party, then press # . |
| Step 3 | Hang up your phone. |
-

Attended Transfer

This feature allows a user to transfer an existing call to another telephone number after first consulting with the dialed party before the user hangs up. Perform the following steps to complete an attended transfer:

Procedure

-
- Step 1** Press the flash button on the telephone handset to put the existing party on hold and get a dial tone.
 - Step 2** Dial the telephone number to which the existing party is being transferred.
 - Step 3** When the callee answers the phone, you may consult with the callee and then transfer the existing party by hanging up your telephone handset.
-

Making a Conference Call in the United States

Procedure

-
- Step 1** Dial the first number.
 - Step 2** When the person you called answers, press the flash or receiver button on the telephone handset. This will put the first person you called on hold and you will receive a dial tone.
 - Step 3** Dial the second person and speak normally when that person answers.
 - Step 4** To conference with both callers at the same time, perform a hook flash.
 - Step 5** To drop the second call, perform a hook flash.
 - Step 6** (Optional) To conference in additional callers, the last person called with a Cisco ATA can call an additional person, that new person can then call someone else, and so on. This is known as *daisy-chaining*.
-

Making a Conference Call in Sweden

Procedure

-
- Step 1** Dial the first number.
 - Step 2** When the person you called answers, press the flash or receiver button on the telephone handset. This will put the first person you called on hold and a dial tone will sound.
 - Step 3** Dial the second person and speak normally when that person answers.
 - Step 4** Perform a hook flash, then press **2** on your telephone keypad to return to the first person. You can continue to switch back and forth between the two callers.

- Step 5** To conference with both callers at the same time, perform a hook flash, then press **3** on the telephone keypad. Once you conference all three callers, the only way to drop a caller is for that caller to hang up.
- Step 6** (Optional) To conference in additional callers, the last person called with a Cisco ATA can call an additional person, that new person can call someone else, and so on. This is known as “daisy-chaining.”
-

Call Waiting in the United States

If someone calls you while you are speaking on the telephone, you can answer by performing a hook flash. You cannot conference in all three callers, but the first person you called could call someone else and daisy-chain them into the conference.

When the Cisco ATA is configured to use Call Waiting by default, press ***70** on your telephone keypad to disable Call Waiting for the duration of the next call.

Call Waiting in Sweden

If someone calls you while you are speaking on the telephone, you can answer by performing a hook flash then pressing **2** on your telephone keypad, or you can conference them with the person to whom you are already speaking by performing a hook flash then pressing **3**. You can also perform a hook flash then press **3** later during the call to create a conference call.

Performing a hook flash then pressing **1** hangs up the first caller and answers the second call. If there is no answer after one minute, the caller receives three beeps and a busy signal.

To enable call waiting for Sweden, press ***43#**. When the Cisco ATA is configured to use Call Waiting by default, press **#43#** to disable Call Waiting for the duration of the next call.

About Call Forwarding

In SIP, the Cisco ATA can control call forwarding and call return.

There are three types of call forwarding:

- Forward Unconditional—Forwards every call that comes in.
- Forward When Busy—Forwards calls when the line is busy.
- Forward on No Answer—Forwards calls when the telephone is not answered after the configured period of 0-63 seconds.

You can activate only one of these services at a time.

Call Forwarding in the United States

Forward Unconditional

Press **#72** on your telephone keypad; enter the number you want to forward call to; then press **#** again.

Forward When Busy

Press **#74** on your telephone keypad; enter the number to forward the calls to; then press **#** again.

Forward On No Answer

Press **#75** on your telephone keypad; enter the number you want to forward the calls to; then press **#** again.

Cancelling Call Forwarding

To cancel call forwarding, press **#73** on your telephone keypad

Call Forwarding in Sweden

Forward Unconditional

Press ***21*** on your telephone keypad; enter the number you want to forward calls to; then press **#**. To cancel, press **#21#**.

Forward When Busy

Press ***67*** on your telephone keypad; enter the number to forward the calls to; then press **#**. To cancel, press **#61#**.

Forward On No Answer

Press ***61*** on your telephone keypad; enter the number you want to forward the calls to; then press **#**. To cancel, press **#67#**.

Forward On No Answer with a Specified Call Forward Delay

Press ***61*** on your telephone keypad; enter the number you want to forward the calls to; then press ***** and the number of seconds for the call forward delay; then press **#** again. To cancel, press **#67#** on your telephone keypad.

Call Return in the United States

Press ***69** on your telephone keypad to activate call return in the United States.

Call Return in Sweden

Press ***69#** on your telephone keypad to activate call return in Sweden.

Calling Line Identification Presentation

Calling Line Identification Presentation (CLIP) shows your identity to callers with Caller ID.

Press ***82** on your telephone keypad to activate CLIP.

About Calling Line Identification Restriction

Calling Line Identification Restriction (CLIR) hides your identity from callers with Caller ID.

Calling Line Identification Restriction in the United States

Press ***67** on your telephone keypad to activate CLIR. This feature is disabled when you hang up.

Calling Line Identification Restriction in Sweden

Press ***31#** on your telephone keypad to activate CLIR. This feature is disabled when you hang up.



Voice Menu Codes

This section contains a quick-reference list of the voice configuration menu options for the Cisco ATA.

This section contains the following tables:

- Cisco ATA Voice Menu Codes—Information Options, page B-1
- Cisco ATA Voice Menu Codes—Configuration Parameters, page B-2
- Cisco ATA Voice Menu Codes—Software Upgrade, page B-4



Note

Follow each voice menu code with #.



Note

The term *Cisco ATA* refers to both the Cisco ATA 186 and the Cisco ATA 188, unless otherwise stated.

Table B-1 lists codes to return basic Cisco ATA information.

Table B-1 Cisco ATA Voice Menu Codes—Information Options

Option	Voice Menu Code	Description
Build information	123123	Build date of the Cisco ATA software
Review IP address	21	Returns IP address of the Cisco ATA
Review MAC address	24	Returns media access control (MAC) address of the Cisco ATA
Review network route IP address	22	Returns IP address of the network route
Review subnet mask	23	Returns subnet mask of the network route
Version number	123	Returns version number of the Cisco ATA software

Table B-2 lists configuration codes.

Table B-2 Cisco ATA Voice Menu Codes—Configuration Parameters

Option	Voice Menu Code	Description
Alternate NTP IP address	78	IP address of the alternate NTP server
Audio mode	312	Allows finer control of the audio component to suit certain user applications
Call features	314	Subscribed features statically enabled by the user
Caller ID method	316	Specifies the signal format when generating the Caller ID format to use
TFTP Configuration Interval	80002	Interval (in seconds) between configuration updates when TFTP configuration is used,
Connection mode	311	Controls the connection mode of the call signaling protocol
Dynamic Host Configuration Protocol (DHCP)	20	Controls whether the Cisco ATA can automatically obtain configuration parameters from a server over the network
DNS 1 IP	916	IP address of the primary DNS server
DNS 2 IP	917	IP address of the secondary DNS server
Encrypt key	320	Encrypts the configuration file on the TFTP server
Num Tx frames	35	Number of frames transmitted per packet
Gatekeeper/proxy server IP address	5	SIP registration proxy server IP address
IP address	1	IP address of the Cisco ATA
LBR codec	300	Low bit rate codec selection
Login ID 0	46	Alternate user ID used for authentication
Login ID 1	47	Alternate user ID used for authentication
Media port	202	Specifies which base port the Cisco ATA uses to receive RTP media streams
Network route address	2	Network router address
NPrintf address	81	IP address of a host to which all Cisco ATA debug messages are sent
NTP server address	141	IP address of the NTP server
Paid features	315	Features subscribed to by the user
Polarity	304	Controls connect and disconnect polarity
PWD 0	4	Password associated with the primary phone line (UID0 or LoginID0)
PWD 1	14	Password associated with the secondary phone line (UID1 or LoginID1)

Table B-2 Cisco ATA Voice Menu Codes—Configuration Parameters (continued)

Option	Voice Menu Code	Description
Rx codec	36	Selects the audio codec type to use to decode received data. The call-receiving station automatically adjusts to the call-initiating station's audio codec type if the call-receiving station supports that audio codec.
Set password	7387277	Configuration interface password
Signal timers	318	Timeout values controlling the starting or stopping of a signaling event
SIP max number of redirects	205	Maximum number of redirections the Cisco ATA will attempt to reach a callee when making a call
SIP NAT IP address	200	WAN IP of the NAT
SIP outbound proxy	206	IP address of the outbound proxy server to which all outgoing SIP requests are sent
SIP port	201	Specifies which port the Cisco ATA listens to for incoming SIP messages
SIP protocol	38	Selects the signaling protocol
SIP registration On	204	Enables SIP registration
SIP registration period	203	Interval (in seconds) between each registration renewal to the SIP registration server
Subnet mask	10	Specifies the subnet mask for the Cisco ATA
TFTP URL	905	IP address of the TFTP server when TFTP configuration is used
Timezone	302	Specifies offset to GMT—used to time-stamp incoming calls for caller ID
ToConfig	80001	Identifies unconfigured or already-configured Cisco ATAs
Trace Fflags	313	Enables logging of debug information
Tx Codec	37	Selects transmitting audio codec preference
UDP TOS bits	255	Determines the precedence and delay of UDP IP packets
UID 0	3	User ID (telephone number) for the PHONE 1 port
UID 1	13	User ID (telephone number) for the PHONE 2 port
Use login ID	93	Determines which pair (UIDx, PWDx or LoginIDx, PWDx) to use for authentication
Use TFTP	305	Enables TFTP as configuration method

Table B-3 lists codes used in the software upgrade process. For information about these codes, see Appendix , “Upgrading the Cisco ATA Signaling Image.”

Table B-3 Cisco ATA Voice Menu Codes—Software Upgrade

Option	Voice Menu Code	Description
Upgrade software	100	Used in the software process to enter the IP address of the PC
Upgrade language to English	101	When upgrading software, changes or upgrades the voice prompt language to English



Cisco ATA Specifications

This section describes Cisco ATA specifications:

- Physical Specifications, page C-1
- Electrical Specifications, page C-2
- Environmental Specifications, page C-2
- Immunity Specifications, page C-2
- Physical Interfaces, page C-3
- Ringing Characteristics, page C-3
- Software Specifications, page C-3
- SIP Compliance Reference Information, page C-5



Note

The term *Cisco ATA* refers to both the Cisco ATA 186 and the Cisco ATA 188, unless otherwise stated.

Physical Specifications

Table C-1 *Physical Specifications*

Description	Specification
Dimensions	1.5 x 6.5 x 5.75 in. (3.8 x 16.5 x 14.6 cm) (H x W x D)
Weight	15 oz (425 g)

Electrical Specifications

Table C-2 *Electrical Specifications*

Description	Specification
Power	0.25 to 7.5W (idle to peak)
DC input voltage	+5.0 VDC at 1.5A maximum
Power adaptor	Universal AC/DC ~3.3 x 2.0 x 1.3 in. (~8.5 x 5.0 x 3.2 cm) ~4.8 oz (135 g) for the AC-input external power adaptor ~4 ft (1.2 m) DC cord 6 ft (1.8 m) cord UL/CUL, CE approved Class II transformer

Environmental Specifications

Table C-3 *Environmental Specifications*

Description	Specification
Operating temperature	41 to 104° F (5 to 40° C)
Storage temperature	–4 to 140° F (–20 to 65° C)
Relative humidity	10 to 90% noncondensing, operating, and nonoperating/storage

Immunity Specifications

EN50082-1, including the following:

- EN61000-3-2, Electromagnetic Compatibility
- EN61000-3-3, Electromagnetic Compatibility
- EN61000-4-2, ESD
- EN61000-4-3, Radiated Immunity
- EN61000-4-4, Burst Transients
- EN61000-4-5, Surge
- EN61000-4-6, Injected RF
- EN61000-4-11, Dips and Sags

Physical Interfaces

Table C-4 Physical Interfaces

Description	Specification
Ethernet	Two RJ-45 connectors, IEEE 802.3 10BaseT standard
Analog telephone	Two RJ-11 FXS voice ports
Power	5 VDC power connector
Indicators	Function button with integrated status indicator Activity LED indicating network activity

Ringing Characteristics

Table C-5 Ringing Characteristics

Description	Specification
Tip/ring interfaces for each RJ-11 FXS port (SLIC)	
Ring voltage	40V _{RMS} (typical, balanced ringing only)
Ring frequency	25 Hz
Ring waveform	Trapezoidal with 1.2 to 1.6 crest factor
Ring load	1400 ohm + 40μF
Ringer equivalence number (REN)	Up to 5 REN per RJ-11 FXS port
Loop impedance	Up to 200 ohms (plus 430-ohm maximum telephone DC resistance)
On-hook/off-hook characteristics	
On-hook voltage (tip/ring)	–50V
Off-hook current	27 mA (nominal)
RJ-11 FXS port terminating impedance option	The Cisco ATA186-I1 and Cisco ATA188-I1 provide 600-ohm resistive impedance. The Cisco ATA186-I2 and Cisco ATA188-I2 provide 270 ohm + 750 ohm // 150-nF complex impedance.

Software Specifications

Table C-6 Software Specifications (All Protocols)

Description	Specification
Call progress tones	Configurable for two sets of frequencies and single set of on/off cadence
Dual-tone multifrequency (DTMF)	DTMF tone detection and generation

Table C-6 Software Specifications (All Protocols) (continued)


Description	Specification
Fax	<p>G.711 fax pass-through and G.711 fax mode.</p> <p>Enhanced fax pass-through is supported on the Cisco ATA. Success of fax transmissions up to 14.4 kbps depends on network conditions, and fax modem/fax machine tolerance to those conditions. The network must have reasonably low network jitter, network delay, and packet-loss rate.</p>
Line-echo cancellation	<ul style="list-style-type: none"> • Echo canceller for each port • 8 ms echo length • Nonlinear echo suppression (ERL > 28 dB for frequency = 300 to 2400 Hz) • Convergence time = 250 ms • ERLE = 10 to 20 dB • Double-talk detection
Out-of-band DTMF	<ul style="list-style-type: none"> • H.245 out-of-band DTMF for H.323 • RFC 2833 AVT tones for SIP, MGCP, SCCP
Configuration	<ul style="list-style-type: none"> • DHCP (RFC 2131) • Web configuration via built-in Web server • Touch-tone telephone keypad configuration with voice prompt • Basic boot configuration (RFC 1350 TFTP Profiling) • Dial plan configuration • Cisco Discovery Protocol
Quality of Service	<ul style="list-style-type: none"> • Class-of-service (CoS) bit-tagging (802.1P) • Type-of-service (ToS) bit-tagging
Security	<ul style="list-style-type: none"> • H.235 for H.323 • RC4 encryption for TFTP configuration files
Voice coder-decoders (codecs)	<p> Note In simultaneous dual-port operation, the second port is limited to G.711 when using G.729.</p> <ul style="list-style-type: none"> • G.723.1 • G.729, G.729A, G.729AB • G.723.1 • G.711A-law • G.711μ-law

Table C-6 Software Specifications (All Protocols) (continued)

Description	Specification
Voice features	<ul style="list-style-type: none">• Voice activity detection (VAD)• Comfort noise generation (CNG)• Dynamic jitter buffer (adaptive)
Voice-over-IP (VoIP) protocols	<ul style="list-style-type: none">• H.323 v2• SIP (RFC 2543 bis)• MGCP 1.0 (RFC 2705)• MGCP 1.0/network-based call signalling (NCS) 1.0 profile• MGCP 0.1• SCCP

SIP Compliance Reference Information

Information on how the Cisco ATA complies with the IETF definition of SIP as described in RFC 2543 is found at the following URL:

<http://www-vnt.cisco.com/SPUniv/SIP/documents/CiscoATASIPComplianceRef.pdf>



SIP Call Flows

This section describes some basic call flows for the Cisco ATA:

- Supported SIP Request Methods, page D-1
- Call Flow Scenarios for Successful Calls, page D-2



Note

The term *Cisco ATA* refers to both the Cisco ATA 186 and the Cisco ATA 188, unless otherwise stated.

Supported SIP Request Methods

The Cisco ATA supports the following SIP request methods:

- INVITE—Indicates a user or service is being invited to participate in a call session.
- ACK—Confirms that the client has received a final response to an INVITE request.
- BYE—Terminates a call and can be sent by either the caller or the callee.
- CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.
- REGISTER—Registers the address listed in the To header field with a SIP proxy.
- NOTIFY—Notifies the user of the status of a transfer using REFER. Also used for remote reset.
- OPTIONS

The following types of responses are used by SIP and generated by the Cisco SIP gateway:

- SIP 1xx—Informational responses
- SIP 2xx—Successful responses
- SIP 3xx—Redirection responses
- SIP 4xx—Client Failure responses
- SIP 5xx—Server Failure responses
- SIP 6xx—Global Failure responses

Call Flow Scenarios for Successful Calls

This section describes call flows for the following scenarios:

- Cisco ATA-to-SIP Server—Registration without Authentication, page D-2
- Cisco ATA-to-SIP Server—Registration with Authentication, page D-3
- Cisco ATA-to-Cisco ATA—Basic SIP to SIP Call without Authentication, page D-6
- Cisco ATA-to-Cisco ATA—Basic SIP to SIP Call with Authentication, page D-12

Each of the call flows includes a call diagram, action descriptions table, and a sample log file.

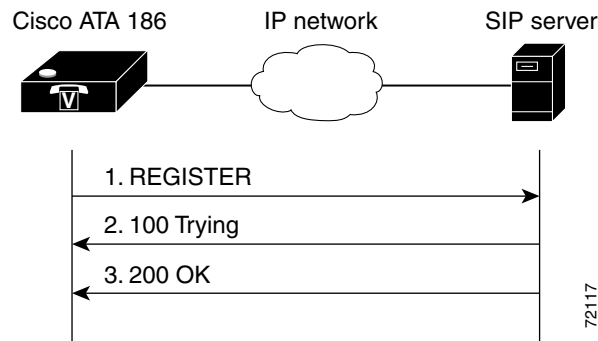
Cisco ATA-to-SIP Server—Registration without Authentication

Figure D-1 illustrates the Cisco ATA registering with the SIP server. Authentication is not required for registration.

The call flow is as follows:

1. Cisco ATA requests registration.
2. Registration is completed.

Figure D-1 Cisco ATA-to-SIP Server—Registration without Authentication



72117

Table D-1 Action Descriptions

Step	Action	Description
Step 1	REGISTER—Cisco ATA to SIP server	Cisco ATA sends a REGISTER message to the SIP server to register the address in the To header field.
Step 2	100 Trying—SIP Server to Cisco ATA	SIP server returns a 100 Trying message, indicating that the REGISTER request has been received.
Step 3	200 OK—SIP server to Cisco ATA	SIP server returns a final 200 OK response, confirming that registration is complete.

Table D-2 Log Listings

1.	REGISTER sip:192.168.2.97 SIP/2.0 Via: SIP/2.0/UDP 192.168.2.194 From: <sip:9301@192.168.2.97;user=phone> To: <sip:9301@192.168.2.97;user=phone> Call-ID: 88397253@192.168.2.194 CSeq: 1 REGISTER Contact: <sip:9301@192.168.2.194;user=phone;transport=udp>;expires=3600 User-Agent; Cisco ATA v2.10 ata186 (0705a) Content-Length: 0
2.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.194 Call-ID: 88397253@192.168.2.194 From: <sip:9301@192.168.2.97;user=phone> To: <sip:9301@192.168.2.97;user=phone> CSeq: 1 REGISTER Content-Length: 0
3.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.194 Call-ID: 88397253@192.168.2.194 From: <sip:9301@192.168.2.97;user=phone> To: <sip:9301@192.168.2.97;user=phone> CSeq: 1 REGISTER Contact: <sip:9301@192.168.2.194;user=phone;transport=udp>;expires="tue, 23 Oct 2001 14:24:57 GMT" Expires: 3600 Content-Length: 0

Cisco ATA-to-SIP Server—Registration with Authentication

Figure D-2 illustrates the Cisco ATA registering with the SIP server. Authentication is required for registration.

The call flow is as follows:

1. Cisco ATA requests registration.
2. SIP server requests authentication credential.
3. Authentication is received and registration is completed.

Figure D-2 Cisco ATA-to-SIP Server—Registration with Authentication

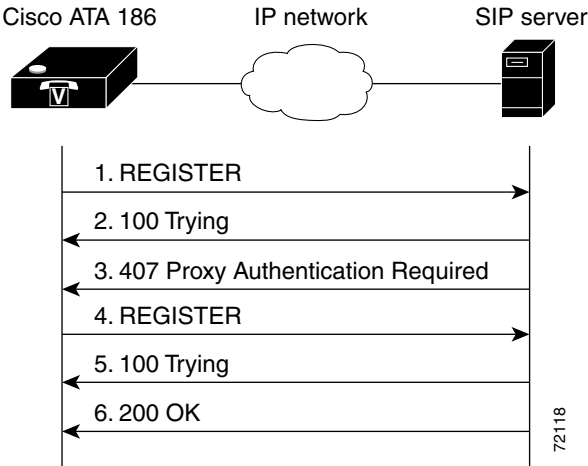


Table D-3 Action Descriptions

Step	Action	Description
Step 1	REGISTER—Cisco ATA to SIP server	Cisco ATA sends a REGISTER message to the SIP server to register the address in the To header field.
Step 2	100 Trying—SIP server to Cisco ATA	SIP server returns a 100 trying message, indicating that the REGISTER request has been received.
Step 3	407 Proxy authentication required— SIP server to Cisco ATA	SIP server returns a request for authentication.
Step 4	REGISTER—Cisco ATA to SIP server	Cisco ATA attempts to register using its authentication credential.
Step 5	100 Trying—SIP server to Cisco ATA	SIP server returns a 100 trying message, indicating that the new REGISTER request has been received.
Step 6	200 OK—SIP server to Cisco ATA	SIP server returns a final 200 OK response, confirming that the authentication credential has been verified and registration is complete.

Table D-4 Log Listings

1.	REGISTER sip:192.168.2.81 SIP/2.0 Via: SIP/2.0/UDP 192.168.2.194 From: <sip:9301@192.168.2.81;user=phone> To: <sip:9301@192.168.2.81;user=phone> Call-ID: 311316842@192.168.2.194 CSeq: 1 REGISTER Contact: <sip:9301@192.168.2.194;user=phone;transport=udp>;expires=3600 User-Agent: Cisco ATA v2.10 ata186 (0705a) Content-Length: 0
2.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.194 Call-ID: 311316842@192.168.2.194 From: <sip:9301@192.168.2.81;user=phone> To: <sip:9301@192.168.2.81;user=phone> CSeq: 1 REGISTER Content-Length: 0
3.	SIP/2.0 407 Proxy Authentication Required Via: SIP/2.0/UDP 192.168.2.194 Call-ID: 311316842@192.168.2.194 From: <sip:9301@192.168.2.81;user=phone> To: <sip:9301@192.168.2.81;user=phone> CSeq: 1 REGISTER Proxy-Authenticate: DIGEST realm="CISCO", nonce="3bd5e334" Content-Length: 0
4.	REGISTER sip:192.168.2.81 SIP/2.0 Via: SIP/2.0/UDP 192.168.2.194 From: <sip:9301@192.168.2.81;user=phone> To: <sip:9301@192.168.2.81;user=phone> Call-ID: 311316842@192.168.2.194 CSeq: 2 REGISTER Contact: <sip:9301@192.168.2.194;user=phone;transport=udp>;expires=3600 User-Agent: Cisco ATA v2.10 ata186 (0705a) Proxy-Authorization: Digest username="9301", realm="CISCO", nonce="3bd5e334", uri="sip:192.168.2.81", response="87ac0afeb08222af706f9e8b5c566ce2" Content-Length: 0
5.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.194 Call-ID: 311316842@192.168.2.194 From: <sip:9301@192.168.2.81;user=phone> To: <sip:9301@192.168.2.81;user=phone> CSeq: 2 REGISTER Content-Length: 0
6.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.194 Call-ID: 311316842@192.168.2.194 From: <sip:9301@192.168.2.81;user=phone> To: <sip:9301@192.168.2.81;user=phone> CSeq: 2 REGISTER Contact: <sip:9301@192.168.2.194;user=phone;transport=udp>;expires="tue, 23 Oct 2001 22:37:56 GMT" Expires: 3600 Content-Length: 0

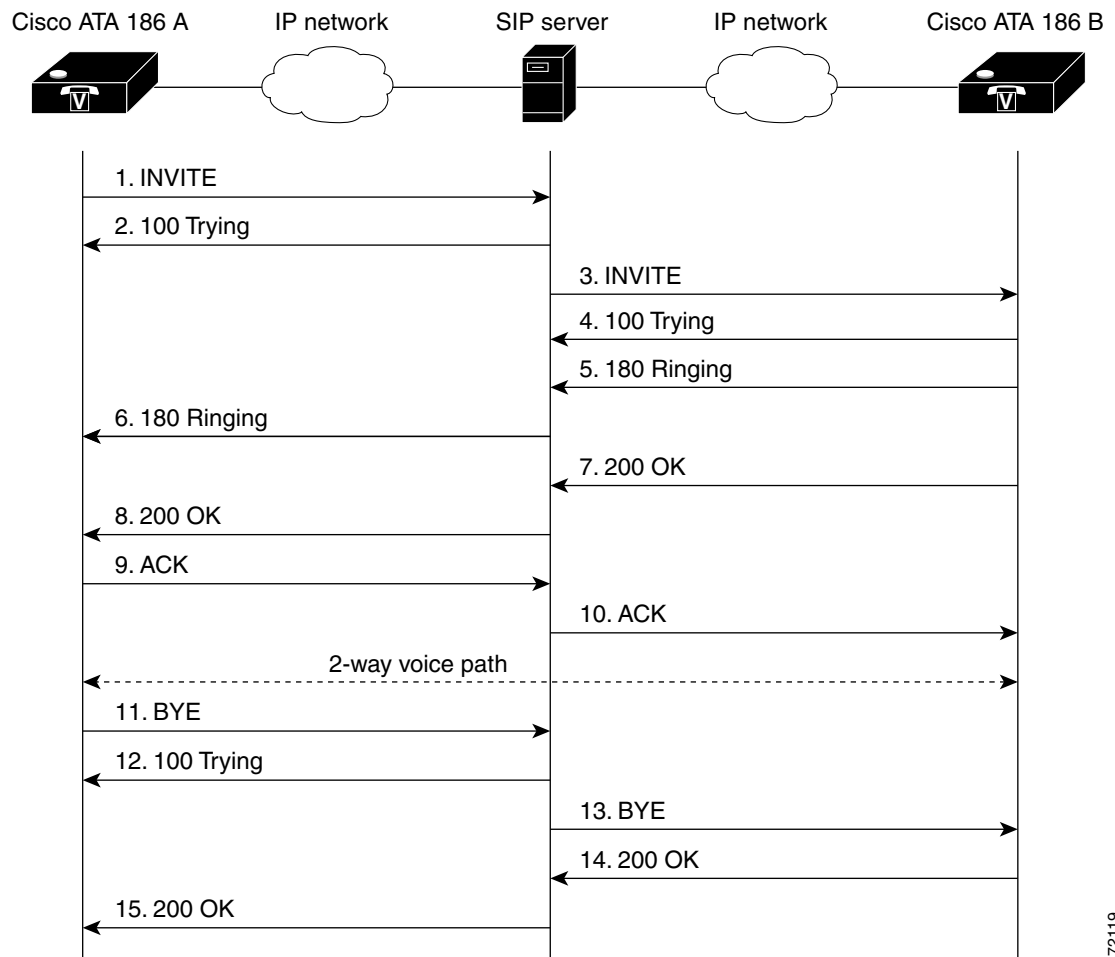
Cisco ATA-to-Cisco ATA—Basic SIP to SIP Call without Authentication

Figure D-3 illustrates a call from one Cisco ATA to another. Authentication by the SIP server is not required.

The call flow is as follows:

1. Call is established between Cisco ATA A and Cisco ATA B.
2. Call is terminated.

Figure D-3 Cisco ATA-to-Cisco ATA—Basic SIP to SIP Call without Authentication



72119

Table D-5 Action Descriptions

Step	Action	Description
Step 1	INVITE—Cisco ATA A to SIP server	Cisco ATA A sends a call session INVITE request to the SIP server to pass on to Cisco ATA B.
Step 2	100 Trying—SIP server to Cisco ATA A	SIP server returns a 100 trying message, indicating that the INVITE request has been received.
Step 3	INVITE—SIP server to Cisco ATA B	SIP server sends the call session INVITE request to Cisco ATA B.
Step 4	100 Trying—Cisco ATA B to SIP server	Cisco ATA B returns a 100 trying message indicating that the INVITE request has been received.
Step 5	180 Ringing—Cisco ATA B to SIP server	Cisco ATA B sends a 180 ringing response to the SIP server to pass on to Cisco ATA A.
Step 6	180 Ringing—SIP server to Cisco ATA A	SIP server sends the 180 ringing response to Cisco ATA A.
Step 7	200 OK—Cisco ATA B to SIP server	Cisco ATA B sends a 200 OK message to the SIP server indicating that a connection has been established.
Step 8	200 OK—SIP server to Cisco ATA A	SIP server passes the 200 OK message to Cisco ATA A.
Step 9	ACK—Cisco ATA A to SIP server	Cisco ATA A sends acknowledgement of the 200 OK response to the SIP server to pass on to Cisco ATA B.
Step 10	ACK—SIP server to Cisco ATA B	SIP server passes ACK response to Cisco ATA B.
A two-way voice path is established between Cisco ATA A and Cisco ATA B.		
Step 11	BYE—Cisco ATA A to SIP server	Cisco ATA A terminates the call session and sends a BYE request to the SIP server indicating that Cisco ATA A wants to terminate the call.
Step 12	100 Trying—SIP server to Cisco ATA A	SIP server returns a 100 trying message indicating that the BYE request has been received.
Step 13	BYE—SIP server to Cisco ATA B	SIP server passes the BYE request to Cisco ATA B.
Step 14	200 OK—Cisco ATA B to SIP server	Cisco ATA B sends a 200 OK message to the SIP server indicating that Cisco ATA B has received the BYE request.
Step 15	200 OK—SIP server to Cisco ATA A	SIP server passes the BYE request to Cisco ATA A.

Table D-6 Log Listings

1.	<pre> INVITE sip:9000@192.168.2.97;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone> Call-ID: 488337201@192.168.3.175 CSeq: 1 INVITE Contact: <sip:8000@192.168.3.175;user=phone;transport=udp> User-Agent: Cisco ATA v2.12 ata186 (0928a) Expires: 300 Content-Length: 253 Content-Type: application/sdp v=0 o=8000 206154 206154 IN IP4 192.168.3.175 s=ATA186 Call c=IN IP4 192.168.3.175 t=0 0 m=audio 10000 RTP/AVP 0 18 8 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:18 G729/8000/1 a=rtpmap:8 PCMA/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 </pre>
2.	<pre> SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.3.175 Call-ID: 488337201@192.168.3.175 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone> CSeq: 1 INVITE Content-Length: 0 </pre>
3.	<pre> INVITE sip:9000@192.168.2.194;user=phone SIP/2.0 Record-Route: <sip:9000@192.168.2.97:5060;user=phone;maddr=192.168.2.97> Via: SIP/2.0/UDP 192.168.2.97:5060;branch=140fed6e-f61cbd1a-52f223b1-9beb149a-1 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone> Call-ID: 488337201@192.168.3.175 CSeq: 1 INVITE Contact: <sip:8000@192.168.3.175;user=phone;transport=udp> User-Agent: Cisco ATA v2.12 ata186 (0928a) Expires: 300 Content-Length: 253 Content-Type: application/sdp v=0 o=8000 206154 206154 IN IP4 192.168.3.175 s=ATA186 Call c=IN IP4 192.168.3.175 t=0 0 m=audio 10000 RTP/AVP 0 18 8 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:18 G729/8000/1 a=rtpmap:8 PCMA/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 </pre>

Table D-6 Log Listings (continued)

4.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.97:5060;branch=140fed6e-f61cbd1a-52f223b1-9beb149a-1 Via: SIP/2.0/UDP 192.168.3.175 Record-Route: <sip:9000@192.168.2.97:5060;user=phone;maddr=192.168.2.97> From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 1 INVITE Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
5.	SIP/2.0 180 Ringing Via: SIP/2.0/UDP 192.168.2.97:5060;branch=140fed6e-f61cbd1a-52f223b1-9beb149a-1 Via: SIP/2.0/UDP 192.168.3.175 Record-Route: <sip:9000@192.168.2.97:5060;user=phone;maddr=192.168.2.97> From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 1 INVITE Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
6.	SIP/2.0 180 Ringing Via: SIP/2.0/UDP 192.168.3.175 Record-Route: <sip:9000@192.168.2.97:5060;user=phone;maddr=192.168.2.97> From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 1 INVITE Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
7.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.97:5060;branch=140fed6e-f61cbd1a-52f223b1-9beb149a-1 Via: SIP/2.0/UDP 192.168.3.175 Record-Route: <sip:9000@192.168.2.97:5060;user=phone;maddr=192.168.2.97> From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 1 INVITE Contact: <sip:9000@192.168.2.194;user=phone;transport=udp> Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 199 Content-Type: application/sdp v=0 o=9000 206275 206275 IN IP4 192.168.2.194 s=ATA186 Call c=IN IP4 192.168.2.194 t=0 0 m=audio 10000 RTP/AVP 0 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15

Table D-6 Log Listings (continued)

8.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.3.175 Record-Route: <sip:9000@192.168.2.97:5060;user=phone;maddr=192.168.2.97 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 1 INVITE Contact: <sip:9000@192.168.2.194;user=phone;transport=udp> Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 199 Content-Type: application/sdp v=0 o=9000 206275 206275 IN IP4 192.168.2.194 s=ATA186 Call c=IN IP4 192.168.2.194 t=0 0 m=audio 10000 RTP/AVP 0 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15
9.	ACK sip:9000@192.168.2.97;user=phone SIP/2.0 Route: <sip:9000@192.168.2.194:5060;user=phone;transport=udp> Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 1 ACK User-Agent: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
10.	ACK sip:9000@192.168.2.194;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.97:5060;branch=140fed6e-f61cbd1a-52f223b1-9beb149a- Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 1 ACK User-Agent: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
11.	BYE sip:9000@192.168.2.97;user=phone SIP/2.0 Route: <sip:9000@192.168.2.194:5060;user=phone;transport=udp> Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 2 BYE User-Agent: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
12.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 19.168.3.175 Call-ID: 488337201@192.168.3.175 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 CSeq: 2 BYE Content-Length: 0

Table D-6 Log Listings (continued)

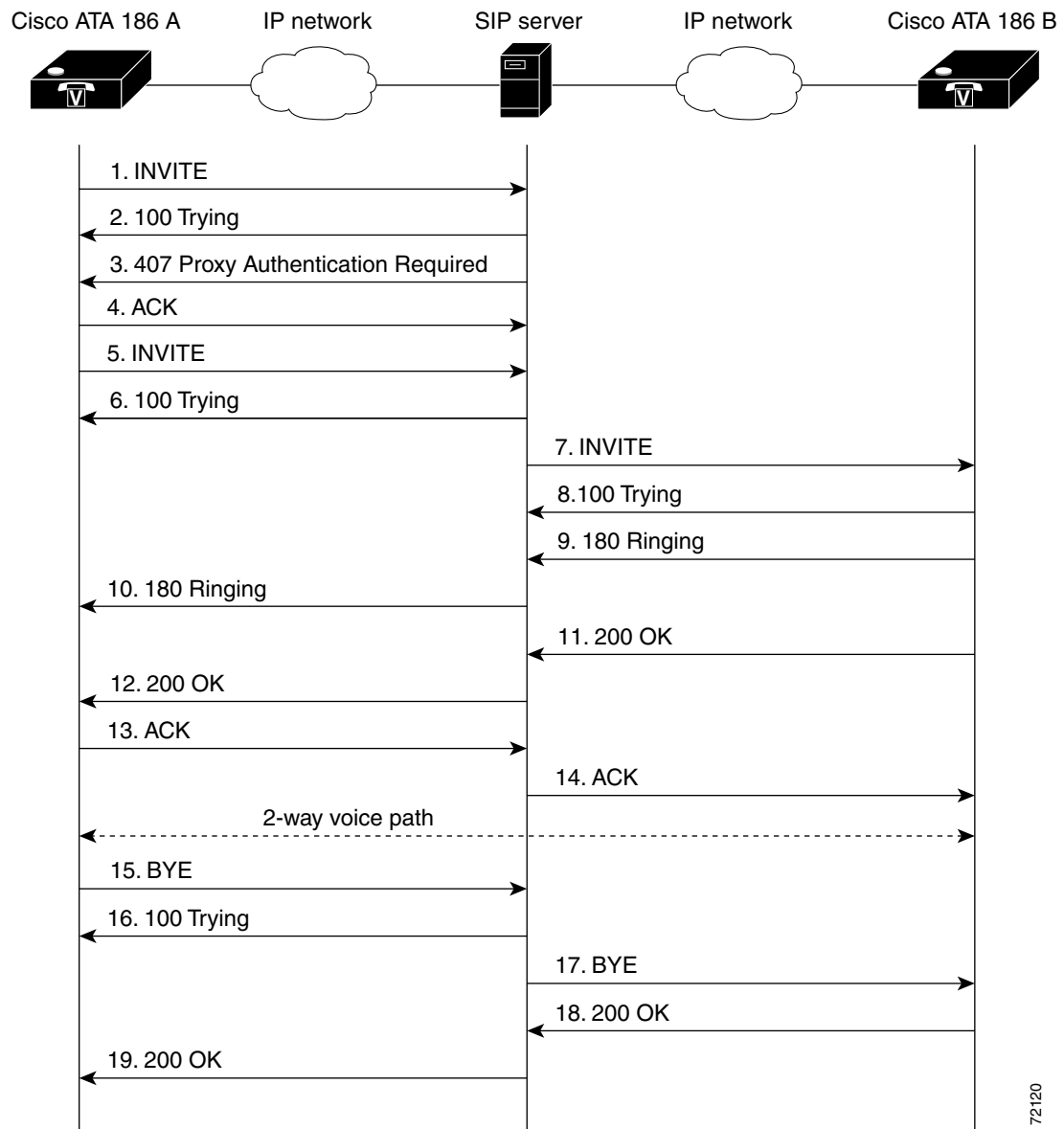
13.	BYE sip:9000@192.168.2.194;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.97:5060;branch=b499b4be-d7995db7-980cd8af-e5ba35f5-1 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 2 BYE User-Agent: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
14.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.97:5060;branch=b499b4be-d7995db7-980cd8af-e5ba35f5-1 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 2 BYE Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
15.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.97;user=phone>;tag=2819471139 To: <sip:9000@192.168.2.97;user=phone>;tag=909616993 Call-ID: 488337201@192.168.3.175 CSeq: 2 BYE Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0

Cisco ATA-to-Cisco ATA—Basic SIP to SIP Call with Authentication

Figure D-4 illustrates a call from one Cisco ATA to another. Authentication by the SIP server is required. The call flow is as follows:

1. Authentication is requested for call initiated by Cisco ATA A.
2. Call is established between Cisco ATA A and Cisco ATA B.
3. Call is terminated.

Figure D-4 Cisco ATA-to-Cisco ATA—Basic SIP to SIP Call with Authentication



72120

Table D-7 Action Descriptions

Step	Action	Description
Step 1	INVITE—Cisco ATA A to SIP server	Cisco ATA A sends a call session INVITE request to the SIP server to pass on to Cisco ATA B.
Step 2	100 Trying—SIP server to Cisco ATA A	SIP server returns a 100 Trying message, indicating that the INVITE request has been received.
Step 3	407 Proxy Authentication Required—SIP server to Cisco ATA A	SIP server returns a request for authentication to Cisco ATA A.
Step 4	ACK—Cisco ATA A to SIP server	Cisco ATA A acknowledges the request for authentication.
Step 5	INVITE—Cisco ATA A to SIP server	Cisco ATA A sends a call session INVITE request along with authentication credential to the SIP server to pass on to Cisco ATA B.
Step 6	100 Trying—SIP server to Cisco ATA A	SIP server returns a 100 Trying message, indicating that the INVITE request has been received.
Step 7	INVITE—SIP server to Cisco ATA B	SIP server sends the call session INVITE request to Cisco ATA B.
Step 8	100 Trying—Cisco ATA B to SIP server	Cisco ATA B returns a 100 trying message indicating that the INVITE request has been received.
Step 9	180 Ringing—Cisco ATA B to SIP server	Cisco ATA B sends a 180 ringing response to the SIP server to pass on to Cisco ATA A.
Step 10	180 Ringing—SIP server to Cisco ATA A	SIP server sends the 180 ringing response to Cisco ATA A.
Step 11	200 OK—Cisco ATA B to SIP server	Cisco ATA B sends a 200 OK message to the SIP server indicating that a connection has been established.
Step 12	200 OK—SIP server to Cisco ATA A	SIP server passes the 200 OK message to Cisco ATA A.
Step 13	ACK—Cisco ATA A to SIP server	Cisco ATA A sends acknowledgment of the 200 OK response to the SIP server to pass on to Cisco ATA B.
Step 14	ACK—SIP server to Cisco ATA B	SIP server passes ACK response to Cisco ATA B.
A two-way voice path is established between Cisco ATA A and Cisco ATA B.		
Step 15	BYE—Cisco ATA A to SIP server	Cisco ATA A terminates the call session and sends a BYE request to the SIP server indicating that Cisco ATA A wants to terminate the call.
Step 16	100 Trying—SIP server to Cisco ATA A	SIP server returns a 100 trying message indicating that the BYE request has been received.
Step 17	BYE—SIP server to Cisco ATA B	SIP server passes the BYE request to Cisco ATA B.
Step 18	200 OK—Cisco ATA B to SIP server	Cisco ATA 186 B sends a 200 OK message to the SIP server indicating that Cisco ATA 186 B has received the BYE request.
Step 19	200 OK—SIP server to Cisco ATA A	SIP server passes the BYE request to Cisco ATA A.

Table D-8 Log Listings

1.	<pre> INVITE sip:9000@192.168.2.81;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone> Call-ID: 557188650@192.168.3.175 CSeq: 1 INVITE Contact: <sip:8000@192.168.3.175;user=phone;transport=udp> User-Agent: Cisco ATA v2.12 ata186 (0928a) Expires: 300 Content-Length: 253 Content-Type: application/sdp v=0 o=8000 177731 177731 IN IP4 192.168.3.175 s=ATA186 Call c=IN IP4 192.168.3.175 t=0 0 m=audio 10000 RTP/AVP 0 18 8 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:18 G729/8000/1 a=rtpmap:8 PCMA/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 </pre>
2.	<pre> SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.3.175 Call-ID: 557188650@192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone> CSeq: 1 INVITE Content-Length: 0 </pre>
3.	<pre> SIP/2.0 407 Proxy Authentication Required Via: SIP/2.0/UDP 192.168.3.175 Call-ID: 557188650@192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To:<sip:9000@192.168.2.81;user=phone>;tag=600eae7-7c3a549a CSeq: 1 INVITE Proxy-Authenticate: DIGEST realm="CISCO", nonce="3bd76584" Content-Length: 0 </pre>
4.	<pre> ACK sip:9000@192.168.2.81:5060 SIP/2.0 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To:<sip:9000@192.168.2.81;user=phone>;tag=600eae7-7c3a549a Call-ID: 557188650@192.168.3.175 CSeq: 1 ACK User-Agent: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0 </pre>

Table D-8 Log Listings (continued)

5.	<pre> INVITE sip:9000@192.168.2.81;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone> Call-ID: 557188650@192.168.3.175 CSeq: 2 INVITE Contact: <sip:8000@192.168.3.175;user=phone;transport=udp> User-Agent: Cisco ATA v2.12 ata186 (0928a) Proxy-Authorization: Digest username="8000",realm="CISCO",nonce="3bd76584", uri="sip:9000@192.168.2.81",response="6e91de67ad976997ffac76f0398ef224" Expires: 300 Content-Length: 253 Content-Type: application/sdp v=0 o=8000 177738 177738 IN IP4 192.168.3.175 s=ATA186 Call c=IN IP4 192.168.3.175 t=0 0 m=audio 10000 RTP/AVP 0 18 8 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:18 G729/8000/1 a=rtpmap:8 PCMA/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 </pre>
6.	<pre> SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.3.175 Call-ID: 557188650@192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone> CSeq: 2 INVITE Content-Length: 0 </pre>
7.	<pre> INVITE sip:9000@192.168.2.194;user=phone SIP/2.0 Record-Route: <sip:9000@192.168.2.81:5060;user=phone;maddr=192.168.2.81 Via: SIP/2.0/UDP 192.168.2.81:5060;branch=c0b3510a-819f9d1a-ea43c345-9604747f-1 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone> Call-ID: 557188650@192.168.3.175 CSeq: 2 INVITE Contact: <sip:8000@192.168.3.175;user=phone;transport=udp> User-Agent: Cisco ATA v2.12 ata186 (0928a) Proxy-Authorization: Digest username="8000",realm="CISCO",nonce="3bd76584", uri="sip:9000@192.168.2.81",response="6e91de67ad976997ffac76f0398ef224" Expires: 300 Content-Length: 253 Content-Type: application/sdp v=0 o=8000 177738 177738 IN IP4 192.168.3.175 s=ATA186 Call c=IN IP4 192.168.3.175 t=0 0 m=audio 10000 RTP/AVP 0 18 8 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:18 G729/8000/1 a=rtpmap:8 PCMA/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 </pre>

Table D-8 Log Listings (continued)

8.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.81:5060;branch=c0b3510a-819f9d1a-ea43c345-9604747f-1 Via: SIP/2.0/UDP 192.168.3.175 Record-Route: <sip:9000@192.168.2.81:5060;user=phone;maddr=192.168.2.81> From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 2 INVITE Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
9.	SIP/2.0 180 Ringing Via: SIP/2.0/UDP 192.168.2.81:5060;branch=c0b3510a-819f9d1a-ea43c345-9604747f-1 Via: SIP/2.0/UDP 192.168.3.175 Record-Route: <sip:9000@192.168.2.81:5060;user=phone;maddr=192.168.2.81> From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 2 INVITE Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
10.	SIP/2.0 180 Ringing Via: SIP/2.0/UDP 192.168.3.175 Record-Route: <sip:9000@192.168.2.81:5060;user=phone;maddr=192.168.2.81> From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 2 INVITE Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
11.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.81:5060;branch=c0b3510a-819f9d1a-ea43c345-9604747f-1 Via: SIP/2.0/UDP 192.168.3.175 Record-Route: <sip:9000@192.168.2.81:5060;user=phone;maddr=192.168.2.81> From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 2 INVITE Contact: <sip:9000@192.168.3.194;user=phone;transport=udp> Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 199 Content-Type: application/sdp v=0 o=9000 179263 179263 IN IP4 192.168.2.194 s=ATA186 Call c=IN IP4 192.168.2.194 t=0 0 m=audio 10000 RTP/AVP 0 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15

Table D-8 Log Listings (continued)

12.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.3.175 Record-Route: <sip:9000@192.168.2.81:5060;user=phone;maddr=192.168.2.81 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 2 INVITE Contact: <sip:9000@192.168.2.194;user=phone;transport=udp> Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 199 Content-Type: application/sdp v=0 o=9000 179263 179263 IN IP4 192.168.2.194 s=ATA186 Call c=IN IP4 192.168.2.194 t=0 0 m=audio 10000 RTP/AVP 0 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15
13.	ACK sip:9000@192.168.2.81;user=phone SIP/2.0 Route: <sip:9000@192.168.2.194:5060;user=phone;transport=udp> Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 2 ACK User-Agent: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
14.	ACK sip:9000@192.168.2.194;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.81:5060;branch=c0b3510a-819f9d1a-ea43c345-9604747f-1 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 2 ACK User-Agent: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
15.	BYE sip:9000@192.168.2.81;user=phone SIP/2.0 Route: <sip:9000@192.168.2.194:5060;user=phone;transport=udp> Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 3 BYE User-Agent: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
16.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 19.168.3.175 Call-ID: 557188650@192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 CSeq: 3 BYE Content-Length: 0

Table D-8 Log Listings (continued)

17.	BYE sip:9000@192.168.2.194;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.81:5060;branch=424f3898-9ef87cec-82179ac3-50eeb1d3-1 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 3 BYE User-Agent: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
18.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.81:5060;branch=424f3898-9ef87cec-82179ac3-50eeb1d3-1 Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 3 BYE Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0
19.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.3.175 From: <sip:8000@192.168.2.81;user=phone>;tag=3515135869 To: <sip:9000@192.168.2.81;user=phone>;tag=100585329 Call-ID: 557188650@192.168.3.175 CSeq: 3 BYE Server: Cisco ATA v2.12 ata186 (0928a) Content-Length: 0



GLOSSARY

Numerics

10BaseT 10-Mbps baseband Ethernet specification using two pairs of twisted-pair cabling (Categories 3, 4, or 5): one pair for transmitting data and the other for receiving data. 10BASET, which is part of the IEEE 802.3 specification, has a distance limit of approximately 328 feet (100 meters) per segment.

A

A-law ITU-T companding standard used in the conversion between analog and digital signals in PCM systems. A-law is used primarily in European telephone networks and is similar to the North American μ -law standard. See also companding and μ -law.

AVT tones Out-of-bound signaling as defined in RFC 2833.

C

category-3 cable One of five grades of UTP cabling described in the EIA/TIA-586 standard. Category 3 cabling is used in 10BaseT networks and can transmit data at speeds up to 10 Mbps.

CED tone detection Called station identification. A three-second, 2100 Hz tone generated by a fax machine answering a call, which is used in the hand-shaking used to set the call; the response from a called fax machine to a CNG tone.

CELP code excited linear prediction compression. Compression algorithm used in low bit-rate voice encoding. Used in ITU-T Recommendations G.728, G.729, G.723.1.

CLIP Calling Line Identification Presentation. Shows your identity to callers with Caller ID.

CLIR Calling Line Identification Restriction. Hides your identity from callers with Caller ID.

CNG Comfort Noise Generation.

codec coder decoder. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm used to compress/decompress speech or audio signals.

companding Contraction derived from the opposite processes of compression and expansion. Part of the PCM process whereby analog signal values are rounded logically to discrete scale-step values on a nonlinear scale. The decimal step number then is coded in its binary equivalent prior to transmission. The process is reversed at the receiving terminal using the same nonlinear scale. Compare with compression and expansion. See also a-law and μ -law.

compression The running of a data set through an algorithm that reduces the space required to store or the bandwidth required to transmit the data set. Compare with companding and expansion.

CoS Class of service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. In SNA subarea routing, CoS definitions are used by subarea nodes to determine the optimal route to establish a given session. A CoS definition comprises a virtual route number and a transmission priority field.

D

DHCP Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

dial peer An addressable call endpoint. In Voice over IP (VoIP), there are two types of dial peers: POTS and VoIP.

DNS Domain Name System. System used on the Internet for translating names of network nodes into addresses.

DSP digital signal processor. A DSP segments the voice signal into frames and stores them in voice packets.

DTMF dual tone multifrequency. Tones generated when a button is pressed on a telephone, primarily used in the U.S. and Canada.

E

E.164 The international public telecommunications numbering plan. A standard set by the ITU-T which addresses telephone numbers.

endpoint A SIP terminal or gateway. An endpoint can call and be called. It generates and/or terminates the information stream.

expansion The process of running a compressed data set through an algorithm that restores the data set to its original size. Compare with companding and compression.

F

firewall Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

FoIP Fax over IP

FQDN Fully Qualified Domain (FQDN) format “mydomain.com” or “company.mydomain.com.”

FSK Frequency shift key.

FXO Foreign Exchange Office. An FXO interface connects to the public switched telephone network (PSTN) central office and is the interface offered on a standard telephone. Cisco FXO interface is an RJ-11 connector that allows an analog connection at the PSTN central office or to a station interface on a PBX.

FXS Foreign Exchange Station. An FXS interface connects directly to a standard telephone and supplies ring, voltage, and dial tone. Cisco's FXS interface is an RJ-11 connector that allows connections to basic telephone service equipment, keysets, and PBXs.

G

G.711 Describes the 64-kbps PCM voice coding technique. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs. Described in the ITU-T standard in its G-series recommendations.

G.723.1 Describes a compression technique that can be used for compressing speech or audio signal components at a very low bit rate as part of the H.324 family of standards. This Codec has two bit rates associated with it: 5.3 and 6.3 kbps. The higher bit rate is based on ML-MLQ technology and provides a somewhat higher quality of sound. The lower bit rate is based on CELP and provides system designers with additional flexibility. Described in the ITU-T standard in its G-series recommendations.

G.729A Describes CELP compression where voice is coded into 8-kbps streams. There are two variations of this standard (G.729 and G.729 Annex A) that differ mainly in computational complexity; both provide speech quality similar to 32-kbps ADPCM. Described in the ITU-T standard in its G-series recommendations.

gateway A gateway allows SIP or H.323 terminals to communicate with terminals configured to other protocols by converting protocols. A gateway is the point where a circuit-switched call is encoded and repackaged into IP packets.

H

H.245 An ITU standard that governs H.245 endpoint control.

H.323 H.323 allows dissimilar communication devices to communicate with each other by using a standard communication protocol. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods.

I

ICMP Internet Control Message Protocol

IP Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.

IVR Interactive voice response. Term used to describe systems that provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words or, more commonly, DTMF signaling.

L

LDAP Lightweight DirectoryAccess Protocol

LEC local exchange carrier.

Location Server A SIP redirect or proxy server uses a location server to get information about a caller's location. Location services are offered by location servers.

M

MGCP Media Gateway Control Protocol.

MWI message waiting indication.

μ-law North American companding standard used in conversion between analog and digital signals in PCM systems. Similar to the European a-law. See also a-law and companding.

N

NAT Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address spaces. Also known as Network Address Translator.

NSE packets Real-Time Transport Protocol (RTP) digit events are encoded using the Named Signaling Event (NSE) format specified in RFC 2833, Section 3.0.

NAT Server Network Address Translation. an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

NTP Network Time Protocol. Protocol built on top of TCP that assures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

P

POTS	Plain old telephone service. Basic telephone service supplying standard single-line telephones, telephone lines, and access to the PSTN.
Proxy Server	An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it.
PSTN	Public switched telephone network.

Q

QoS	Quality of Service. The capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.
------------	---

R

Redirect Server	A redirect server is a server that accepts a SIP request, maps the address into zero or more new addresses, and returns these addresses to the client. It does not initiate its own SIP request nor accept calls.
Registrar Server	A registrar server is a server that accepts Register requests. A registrar is typically co-located with a proxy or redirect server and may offer location services.
router	Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information. Occasionally called a gateway (although this definition of gateway is becoming increasingly outdated). Compare with gateway.
RTP	Real-Time Transport Protocol. One of the IPv6 protocols. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides services such as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.

S

SCCP	Signaling connection control part.
SDP	Session Definition Protocol. An IETF protocol for the definition of Multimedia Services. SDP messages can be part of SGCP and MGCP messages.

SIP	Session Initiation Protocol. Protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.
SIP endpoint	A terminal or gateway that acts as a source or sink of Session Initiation Protocol (SIP) voice data. An endpoint can call or be called, and it generates or terminates the information stream.
SLIC	Subscriber Line Interface Circuit. An integrated circuit (IC) providing central office-like telephone interface functionality.
SOHO	Small office, home office. Networking solutions and access technologies for offices that are not directly connected to large corporate networks.

T

TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
TFTP	Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).
TN power systems	A TN power system is a power distribution system with one point connected directly to earth (ground). The exposed conductive parts of the installation are connected to that point by protective earth conductors.
TOS	Type of service. See CoS.

U

UAC	User agent client. A client application that initiates the SIP request.
UAS	User agent server (or user agent). A server application that contacts the user when a SIP request is received, and then returns a response on behalf of the user. The response accepts, rejects, or redirects the request.
UDP	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
user agent	See UAS.

V

VAD	Voice activity detection. When enabled on a voice port or a dial peer, silence is not transmitted over the network, only audible speech. When VAD is enabled, the sound quality is slightly degraded but the connection monopolizes much less bandwidth.
------------	--

voice packet gateway

Gateway platforms that enable Internet telephony service providers to offer residential and business-class services for Internet telephony.

VoIP

Voice over IP. The capability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. VoIP is a blanket term, which generally refers to Cisco's standard-based (for example H.323) approach to IP voice traffic.

X**XML**

eXtensible Markup Language. Designed to enable the use of SGML on the World-Wide Web. XML allow you to define your own customized markup language.



Numerics

- 486 Busy Here response-timeout configuration 5-26
- 802.1Q VLAN ID 3-3, 5-35

A

- account information parameters 5-9
- Action Identifiers 6-4
- advanced audio configuration 4-4
- AlertTone 5-47
- alphanumeric values 3-17
- alternate gatekeeper requirement configuration setting 5-28
- alternate NTP IP address configuration 5-31
- AltGk parameter 4-10, 5-13
- AltNTPIP parameter 5-31
- ata.txt file 3-9
- atadefault.cfg configuration file 3-12
- atadefault.cfg file 3-11
- atapname.exe Tool 3-10
- ata unique configuration file 3-3, 3-12
- audio and call waiting tone mixing 4-5
- audio and call-waiting tone mixing 5-29
- audio configuration 4-4
- AudioMode parameter 5-20, 7-2, 7-6
- audio operating mode 5-20
- authentication 4-2, 5-12
- authentication ID 5-11

B

- backup proxy configuration parameter 5-13

- backup-server parameters 5-13
- Bellcore (FSK) method 5-23
- Bellcore method for called ID 5-25
- billable features 4-4
- billable features configuration 4-4
- binary configuration file creation 3-9
- blind-transfer configuration setting 5-23, 5-24
- bootload
 - process 3-2
- BusyTone 5-45

C

- CallCmd parameter 5-47
- Call Command behavior 6-7
- call commands
 - changing A-1
- caller ID A-2
- caller ID configuration setting 5-23
- caller-ID-configuration setting 5-24
- caller ID format 5-25
- CallerIdMethod parameter 5-25
- call features 5-23
- CallFeatures parameter 5-23
- call forwarding
 - in Sweden A-6
 - in United States A-5
 - types A-5
- call forwarding configuration setting 5-29
- calling line identification presentation (CLIP) A-6
- calling line identification restriction
 - definition A-6
 - in Sweden A-7

- in United States **A-7**
- call-progress tone parameters **5-42, 5-44**
- Call-progress tones **4-8**
- call return
 - in Sweden **A-6**
 - in United States **A-6**
- call return configuration setting **5-23**
- call-return configuration setting **5-24**
- call waiting **4-10**
 - in Sweden **A-5**
 - in United States **A-5**
- call-waiting caller ID **A-2**
- call-waiting-caller ID configuration setting **5-24**
- call-waiting caller ID setting **5-23**
- call-waiting configuration setting **5-23, 5-24**
- call-waiting period **5-33**
- call waiting tone **4-5**
- call waiting tone and audio mixing **4-5**
- CallWaitTone **5-46**
- CDP discovery setting **5-34**
- cfgfmt.exe tool **3-9, 3-11**
- CfgInterval parameter **3-2, 5-5**
- Cisco ATA route static configuration **5-7**
- Cisco ATA-specific configuration file **3-3**
- Cisco CallManager environment configuration setting **5-28**
- Cisco Discovery Protocol (CDP) **3-2**
- CLIP_CLIR **5-23**
- CLIP_CLIR setting **5-23, 5-24**
- codec negotiation in sending fax **5-28**
- codecs **4-3**
- codec setting **4-3**
- Comfort **4-5**
- common parameters
 - configuration **3-8**
- conference call
 - in Sweden **A-4**
 - in United States **A-4**
- configuration
 - advanced audio **4-4**
 - alphabetical listing of features with related parameters **4-12**
 - atadefault.cfg file **3-11**
 - audio **4-4**
 - authentication **4-2**
 - billable features **4-4**
 - cfgfmt.exe tool **3-9, 3-11**
 - codec **4-3**
 - dial plan **4-6**
 - features and related parameters **4-12**
 - hook flash timing **4-5**
 - methods
 - using TFTP and DHCP servers **3-7, 3-8**
 - Web-based **3-18, 3-20**
 - Wed-based **3-21**
 - mixing of call waiting tone and audio **4-5**
 - NAT/PAT translation **4-7**
 - NAT gateway **4-7**
 - network timing **4-8**
 - on-hook delay **4-5**
 - OutBoundProxy support **4-8**
 - parameters
 - AltGk **4-10, 5-13**
 - AltNTPIP **5-31**
 - AudioMode **5-20, 7-2, 7-6**
 - CallCmd **5-47**
 - CallerIdMethod **5-25**
 - CallFeatures **5-23**
 - CfgInterval **3-2, 5-5**
 - ConnectMode **5-28, 7-3**
 - DHCP **5-7**
 - DialPlan **5-38**
 - DNS1IP **5-31**
 - DNS2IP **5-31**
 - EncryptKey **3-11, 5-6, 9-5**
 - FeatureTimer **5-26**
 - Gateway **5-11**
 - Gateway2 **5-11**

GkId 5-14
 GkOrProxy 4-2, 4-10, 5-10
 GkTimeToLive 5-14
 IPDialPlan 5-38
 LBRCodec 5-20
 LoginID0 5-12
 LoginID1 5-12
 MAXRedirect 4-2, 5-15
 MediaPort 4-7, 5-17
 MediaPort parameter 4-2
 NATIP 4-2, 4-7, 5-16, 5-29
 NatServer 5-18
 NatTimer 5-19
 network timing 4-8
 NPrintF 5-36
 NTPIP 5-30
 NumTxFrames 5-22
 OpFlags 5-34
 OutBoundProxy 4-2, 4-8, 5-17
 Polarity 5-27
 PWD0 5-9
 PWD1 5-10
 RingOnOffTime 5-37
 RxCodec 5-21
 SigTimer 5-32
 SIPPort 4-7, 5-17
 SIPPort parameter 4-2
 SIPRegInterval 4-2, 5-15
 SIPRegOn 4-2, 5-16
 StaticIp 5-7
 StaticNetMask 5-8
 StaticRoute 4-7, 5-7
 TftpURL 5-5
 TimeZone 5-30
 ToConfig 5-4
 TraceFlags 5-36
 TxCodec 5-22
 UDPTOS 5-32
 UID0 5-9

UID1 5-9
 UIPassword 5-3, 9-5
 UseLoginID 5-11
 UseSIP 5-14
 VLAN Setting 5-35
 refresh interval 4-3
 repeat dialing on busy signal 4-9
 required parameters 4-1
 services and related parameters 4-12
 silence suppression 4-5
 SIP proxy server redundancy 4-10
 timeout on no answer for call forwarding 4-10
 timing 4-8
 VIA header 4-9
 configuration changes taking effect 3-6
 configuration-complete configuration parameter 4-2
 configuration-complete parameter 5-4
 configuration in a non-TFTP server environment 3-6
 configuration in a TFTP server environment 3-5
 configuration-method parameters 5-4
 configuration update interval 5-5
 configuring seconds between registration renewal 4-2
 ConnectMode parameter 5-28, 7-3
 Context-Identifiers 6-3, 6-4
 converting MAC address to hexadecimal format 3-10
 convert unique configuration file to binary format 3-5
 creating a text configuration file 3-8

D

datagram precedence 5-32
 debugging 9-4
 debugging, preserv.exe program 9-4
 debugging diagnostics
 TraceFlags 4-5
 default call waiting state 5-29
 default configuration file 3-12
 default values 3-8, 5-2
 device hostname 5-35

DHCP

- disabling 5-7
- enabling 5-7
- DHCP discovery message 5-34
- DHCP option 12 5-35
- DHCP option 150 3-13, 5-34
- DHCP option 66 3-13
- DHCP options 3-14
- DHCP parameter 5-7
- DHCP server
 - configuration without using DHCP 3-15
 - if not under control of Cisco ATA administrator 3-14
- DHCP server-supplied TFTP configuration filename used
 - configuration setting 5-34
- DHCP server usage 3-13
- diagnostics 4-5
- DialPlan 4-6
 - dial plan blocking 5-41
- Dial Plan Commands 5-39
- dial plan configuration 4-6
- dial plan examples 5-40
- DialPlan parameter 5-38
- dial plans 5-38
- dial plan syntax 5-39
- DialTone 5-44
- direct IP-to-IP calls 4-11
- disabling access to Web interface 4-6
- disabling CDP discovery 3-3
- disabling use of DHCP server 3-16
- disabling VLAN encapsulation 3-3
- disabling VLAN IP encapsulation 3-3
- display of hardware information 4-7
- DNS1IP parameter 5-31
- DNS2IP parameter 5-31
- DNS lookup 5-29
- DNS SRV lookup 4-6
- DNS SRV support 4-6
- downloading Cisco ATA software from CCO 3-6, 3-7
- DTMF Method

- always out-of-band setting 5-21
- by negotiation 5-21
- in band setting 5-21

- DtmfMethod configuration settings 5-21
- DTMF method for caller ID 5-25
- dummy packets for NAT 5-18
- dynamic payload type 5-28

E

- electrical specifications C-2
- enabling SIP registration 4-2
- enabling user-specified voice VLAN ID 3-3
- encryption 3-11
- encryption key 5-6
- EncryptKey 3-11
- EncryptKey parameter 5-6, 9-5
- entering alphanumeric values 3-17
- environmental specifications C-2
- establishing IP connectivity 3-15
- Ethernet ports 1-6
- example_uprofile.txt file 3-9
- example_uprofile.txt sample configuration file 3-8
- example_uprofile.txt text file 5-2
- example configuration text file 5-2

F

- factory default reset 3-18
- failback to primary proxy 5-13
- fax CED tone detection configuration setting 5-21
- fax mode 7-1, 7-6
 - configuration
 - per-call basis 7-7
 - G.711 codec only setting 5-23, 5-24
 - no fax tone detection setting 5-23, 5-24
 - no silence suppression setting 5-23, 5-24
- fax mode configuration 7-6, 7-7

fax mode configuration settings **5-23**
 fax-mode configuration settings **5-24**
 fax pass-through **5-28**
 G.711μ-law **5-28**
 G.711 A-law **5-28**
 fax pass-through mode **7-1**
 fax pass-through mode, enabling **7-4, 7-5**
 fax Pass-through mode configuration **7-2**
 fax pass-through redundancy configuration setting **5-28**
 fax relay, disabling **7-5**
 fax services **7-1**
 fax services, debugging **7-7, 7-9**
 features and related parameters **4-12**
 FeatureTimer parameter **5-26**
 forgotten password **5-3**
 forward-on-busy setting **5-23, 5-24**
 forward-on-no-answer setting **5-23, 5-24**
 forward-unconditionally setting **5-23, 5-24**
 frames per packet configuration **5-22**
 frequently asked questions **9-5**
 Function button **8-1, 9-1**
 function button **1-6, 3-3**
 FXS ports **1-6**

G

G.711 silence suppression configuration **5-21**
 G.723.1 **5-20**
 G.729 **5-20**
 Gateway2 parameter **5-11**
 Gateway parameter **5-11**
 generating binary configuration file **3-9**
 GkId parameter **5-14**
 GkOrProxy parameter **4-2, 4-10, 5-10**
 GkTimeToLive parameter **5-14**
 Greenwich Mean Time offset **5-30**

H

h245 tunneling configuration setting **5-28**
 hardware information display **4-7**
 hook flash time **5-33**
 hook-flash timing **4-5**
 hook flash timing configuration **4-5**
 Hotline/Warmline **5-41**
 HTTP refresh **5-34**
 HTTP reset **5-34**

I

immunity specifications **C-2**
 include command **3-9**
 installation
 procedure **2-3**
 IP address static configuration **5-7**
 IP dial plan configuration **5-38**
 IPDialPlan parameter **5-38**
 IP precedence (ToS bit) of UDP packets **5-32**
 ITU G.711 **4-5**

L

LBRCodec parameter **5-20**
 Lightweight Directory Access Protocol (LDAP) **1-3**
 line polarity **5-27**
 LoginID0 parameter **5-12**
 LoginID1 parameter **5-12**
 log listings **D-3, D-5, D-8, D-14**
 low-bit-rate codec **5-21**
 low-bit-rate codecs **5-20**

M

MAC address **3-10**
 making configuration changes after boot up **3-10**

maximum number of digits in phone number **5-25**
 maximum number of times to try redirection **4-2**
 maximum redirects to another number **5-15**
 MAXRedirect parameter **4-2, 5-15**
 MediaPort **4-7**
 MediaPort parameter **4-2, 5-17**
 message-waiting-indication setting **5-23, 5-24**
 methods supported **1-9**
 mixing of call waiting tone and audio **4-5**

N

NAT/PAT translation **4-7**
 NAT/PAT translation configuration **4-7**
 NAT gateway configuration **4-7**
 NATIP **4-7**
 NATIP parameter **4-2, 5-16, 5-29**
 NatServer parameter **5-18**
 NatTimer parameter **5-19**
 Network Address Translation (NAT) **4-7, 5-18**
 network parameters **5-6**
 network requirements **2-2**
 network timing **4-8**
 network timing configuration **4-8**
 no-answer timeout **5-33**
 non-dotted hexadecimal MAC address location **3-9**
 normal start connection mode setting **5-28**
 NPrintf **4-5**
 NPrintf parameter **5-36**
 NTP IP address configuration **5-30**
 NTPIP parameter **5-30**
 NumTxFrames parameter **5-22**

O

obtaining non-dotted hexadecimal MAC address of Cisco
 ATA **3-9**
 on-hook delay **4-5**
 on-hook delay before call is disconnected **5-26**

on-hook delay configuration **4-5**
 operating parameters **5-19**
 OpFlags parameter **5-34**
 optional feature parameters **5-35**
 OutBoundProxy parameter **4-2, 4-8, 5-17**
 outbound proxy server **5-17**
 OutBoundProxy support configuration **4-8**

P

paid features **5-24**
 parameters and defaults **xii, 5-1**
 parameters for configuration method **5-4**
 parameter types **5-1**
 password **5-3**
 password for Phone 1 port **5-9**
 password for Phone 2 port **5-10**
 physical interfaces **C-3**
 physical specifications **C-1**
 placing call without using SIP proxy **4-11**
 polarity **5-27**
 Polarity parameter **5-27**
 polarity reversal before and after Caller ID signal **5-25**
 polarity reversal before and after caller ID signal **5-25**
 port
 incoming SIP requests **5-17**
 outgoing SIP requests **5-17**
 RTP media **5-17**
 port for debug messages
 configuration **5-36**
 port for incoming SIP requests **4-2**
 primary domain name server IP address **5-31**
 Private Line Automatic Ringdown (PLAR) **5-41**
 Progress Indicator configuration setting **5-28**
 progress tones **4-8**
 proxy server **1-4**
 proxy server for all outbound SIP requests **4-2**
 prserv **7-9**
 PWD0 parameter **5-9**

PWD1 parameter 5-10

R

received= tag in VIA header 5-29
 receiving-audio codec settings 5-21
 redialing timeout 5-26
 redirection attempts 4-2
 redirect server 1-4
 redirects to another number 5-15
 redundancy 5-31
 refreshing the Cisco ATA 3-22
 refresh interval 4-3, 5-5
 refresh-interval configuration 3-5
 refresh procedure 3-10
 REGISTER message configuration 5-29
 registrar address 4-2
 registrar server 1-4
 registration-renewal configuration setting 5-28
 registration renewal increment 5-15
 registration server 5-10
 registration with authentication D-3
 registration without authentication D-2
 reorder delay 5-33
 Reorder Tone 5-45
 repeat dialing on busy signal 4-9
 request high reliability 5-32
 request high throughput 5-32
 request low delay 5-32
 required parameters 4-1
 resetting the Cisco ATA 3-22
 resetting the Cisco ATA to factory defaults 3-18
 retry timeout 5-26
 reviewing default router for Cisco ATA to use 3-17
 reviewing subnet mask of Cisco ATA 3-17
 review IP address of Cisco ATA 3-16
 Ringback Tone 5-46
 ringback tone configuration setting 5-29
 ringer cadence pattern configuration 5-37

ringing characteristics C-3

ring loads 9-5

RingOnOffTime 5-37

RingOnOffTime parameter 5-37

ring timeout 5-33

RJ-45 LED

Cisco ATA 186 1-6

Cisco ATA 188 1-6

rtptcatch 7-12, 7-13, 7-15, 7-16, 7-17, 7-19

RTP frames 7-12

RTP media port 4-2, 5-17

RTP packets 7-12

RTP payload type 5-28

RTP statistics 7-12

RxCodec parameter 5-21

S

safety recommendations 2-2

sample configuration text file 3-8

scaling factor calculation 5-43

secondary domain name server IP address 5-31

send special character O 5-25

send special character P 5-25

services

basic 1-8

supplemental 1-10

services and related parameters 4-12

setting a password 5-3

setting the codec 4-3

signaling image upgrade 3-22

SigTimer parameter 5-32

silence suppression 4-5

SIP 1-2, 1-3

advanced features 4-3

call flow scenarios D-2

clients 1-4

parameters 5-14

request methods D-1

servers **1-4**
 SIP call return configuration setting **5-29**
 SIP mode configuration parameter **4-2**
 SIP mode parameter **5-14**
 SIPPort **4-7**
 SIPPort parameter **4-2, 5-17**
 SIP proxy not used for call **4-11**
 SIP proxy server address **4-2**
 SIP proxy server configuration parameter **5-10**
 SIP Proxy Server redundancy **4-10**
 SIPRegInterval parameter **4-2, 5-15**
 SIP registration **4-2**
 SIP registration enabled **5-16**
 SIPRegOn parameter **4-2, 5-16**
 SIP to SIP call with authentication **D-12**
 SIP to SIP call without authentication **D-6**
 software download from CCO **3-6, 3-7**
 software specifications (all protocols) **C-3**
 specifying a preconfigured VLAN ID **3-3**
 specifying VLAN CoS bit value (802.1P priority) for UDP packets **3-3**
 specifying VLAN CoS bit value for TCP packets **3-3**
 standard payload type **5-28**
 statically configuring various IP addresses **3-2**
 StaticIP **3-15**
 StaticIP parameter **5-7**
 StaticNetMask **3-15**
 StaticNetMask parameter **5-8**
 static network-router-probing configuration setting **5-34**
 StaticRoute **3-15, 4-7**
 StaticRoute parameter **5-7**
 stuttering dial tone **4-10**
 subnet mask static configuration **5-8**
 supplementary services
 cancelling **A-1**
 common **A-1**

T

TFTP server IP address **3-13**
 TFTP server IP address or URL specification **5-5**
 TFTP server name **3-13**
 TFTP server usage **5-4**
 TftpURL parameter **5-5**
 three-way calling configuration setting **5-23**
 three-way-calling configuration setting **5-24**
 timeout configuration for failback **5-13**
 timeout on no answer for call forwarding **4-10**
 timeouts
 redialing **5-26**
 retry **5-26**
 time-stamping incoming calls **5-30**
 time zone configuration **5-30**
 TimeZone parameter **5-30**
 timing configuration **4-8**
 ToConfig parameter **5-4**
 tones **4-8**
 trace-features configuration **5-36**
 TraceFlags parameter **5-36**
 transfer with consultation **5-23**
 transfer-with-consultation configuration setting **5-24**
 transmitting-audio codec settings **5-22**
 troubleshooting
 general tips **9-1**
 installation **9-3**
 upgrade issues **9-3**
 two-way cut-through configuration setting **5-28**
 TxCodec parameter **5-22**

U

UDPTOS parameter **5-32**
 UID0 parameter **5-9**
 UID1 parameter **5-9**
 UIPassword parameter **5-3, 9-5**
 UIPassword prompt configuration setting **5-35**

- unconditional call forwarding **4-10**
- unique configuration file **3-9, 3-12**
- upgrading firmware from TFTP server **8-1**
- upgrading software
 - using executable file **8-2**
- upgrading software from TFTP server **8-1**
- upgrading the signaling image **3-22**
- UseLoginID parameter **5-11**
- User agent client (UAC) **1-3**
- User agent server (UAS) **1-3**
- user configurable timeout **4-10**
- User ID **5-9**
- User Interface (UI) Parameters **5-3**
- UseSIP parameter **5-14**
- UseTFTP parameter **5-4**
- circuit breaker (15A) **2-5**
- installation **2-2**
- lightning activity **2-2**
- main disconnecting device **2-2**
- No. 26 AWG **2-5**
- product disposal **2-2**
- web configuration disabling **5-34**
- Web interface access disabled **4-6**

V

- VIA header **4-9**
- VLAN CoS bit value (802.1P priority) for TCP packets **5-35**
- VLAN CoS bit value (802.1P priority) for UDP packets **5-35**
- VLAN ID **5-35**
- VLAN ID example **3-4**
- VLAN IP encapsulation setting **5-34**
- VLAN-related parameters **3-3**
- VLAN Setting parameter **5-35**
- VLAN tagging **3-2**
- voice configuration menu **3-16**
- Voice Menu Codes
 - configuration parameters **B-2**
 - information options **B-1**
 - software upgrade **B-4**

W

- WAN address of attached router/NAT **4-2, 5-16**
- warnings

