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 4-23—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 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 5-19	Integer	Seconds between registration renewal	203	1	86400	3600
MAXRedirect, page 5-20	Integer	Maximum number of times to try redirection	202	0	10	5
SIPRegOn, page 5-20	Integer	Enable SIP registration	204	0	1	0
NATIP, page 5-21	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 5-19	Integer	Port to listen for incoming SIP requests	201	1	65535	5060
MediaPort, page 5-30	Integer	Base port to receive RTP media; only used to support SIP behind a NAT	202	1	65535	16384
SipOutBoundProxy, page 5-21	Alphanumeric string	Proxy server for all outbound SIP requests. All SIP requests are sent to SipOutBoundProxy, when configured, instead of to the configured GkOrProxy.	206	—	—	0
GkOrProxy, page 5-13	Alphanumeric string	SIP proxy server address or registrar address.	5	—	—	0

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 5-18
- UID0, page 5-15
- UID1, page 5-16
- LoginID0, page 5-17
- LoginID1, page 5-18
- PWD0, page 5-16
- PWD1, page 5-17

Setting the Codec

The LBRCodec (low-bit-rate codec) parameter determines whether the G.723, G.726 or G.729A codec, in addition to G.711A-law and G.711µ-law, can be used for receiving and transmitting. For configuration information, see the "LBRCodec" section on page 5-32.

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 5-6.

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

The TOS (specifies the precedence and delay of audio and signaling IP packets) and AudioMode (audio operating mode) parameters allow you to tune audio configuration.

Related Parameters

TOS, page 5-34

AudioMode, page 5-32

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 5-36, CallFeatures, page 5-35
Call Forwarding	PaidFeatures, page 5-36, CallFeatures, page 5-35, ConnectMode, page 5-41, SigTimer, page 5-40
Call Transfer	PaidFeatures, page 5-36, CallFeatures, page 5-35

Table 4-2 Billable Features and Related Parameters (continued)

Feature	Related Parameters
Call Waiting	PaidFeatures, page 5-36, CallFeatures, page 5-35, SigTimer, page 5-40
Caller ID	PaidFeatures, page 5-36, CallFeatures, page 5-35, CallerIdMethod, page 5-49
Call Return	ConnectMode, page 5-41, PaidFeatures, page 5-36, CallFeatures, page 5-35
Polarity	Polarity, page 5-51
Voice Mail Indicator	PaidFeatures, page 5-36, CallFeatures, page 5-35

Note CallWaitCallerID is an obsolete parameter. Do not use it.

Call Forwarding Setting Removal Using HTTP

The service provider can remotely reset a call forwarding setting for which a subscriber configured an incorrect phone number to receive fowarded calls.

The service provider issues the following command, which removes call forwarding settings for both Cisco ATA phone lines:

`http://ipaddress/resetcfwd/`

where *ipaddress* is the IP address of the Cisco ATA whose call forwarding numbers are being removed.

This Web page is password protected. Once the service provider issues this command, this Web page shows that the current call-waiting and call-forwarding settings are *N/A*.

Call-Waiting Hang-Up Alert

This feature provides an audible alert (ringtone) whenever the user inadvertently hangs up from a call-waiting call while an active call is still on hold.

This section contains the following topics:

- Enabling the Call-Waiting Hang-Up Alert Feature, page 4-6
- Default Behavior of Call-Waiting Calls, page 4-6

Enabling the Call-Waiting Hang-Up Alert Feature

To enable the call-waiting hang-up alert feature, perform the following steps:

Procedure

Step 1 Enable bit 25 of the Cisco ATA ConnectMode parameter. (For more information, see the "ConnectMode" section on page 5-41.

Step 2 Make sure the call-waiting call command is set to one of the following values:

- Kf;EFh;HF; (for U.S. users)
- Kh;HFf;EF; (for U.S. users)
- Kf1;HFf2;EFf3;AFf4;HQh;HF; (for Sweden users)

Note The *F* Action-Identifier specifies the retrieval of the held call after the active call is disconnected when the user hangs up. For more information about call commands, see Chapter 6, "Call Commands."

Default Behavior of Call-Waiting Calls

Without the call-waiting hang-up alert feature enabled, both the call-waiting call and active call are disconnected as soon as the user hangs up the phone.

To check whether this default behavior is in effect, search for the appearance of the string *h;HH* within the sequence of call-waiting call commands. The context-identifier *K* denotes the beginning of the call-waiting call commands.

With this default behavior, the call-waiting call command string could be one of the following examples:

- Kf;EFh;HH; (for U.S. users)
- Kh;HHf;EF; (for U.S. users)
- Kf1;HFf2;EFf3;AFf4;HQh;HH; (for Swedish users)
- Kf1;HFf2;EFf3;AFf4;HQ; (for Swedish users with no specific on-hook treatment defined)

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

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 5-32—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 5-40—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 5-41—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 5-38—Bits 8 to 12

Configurable Reboot of Cisco ATA

The Cisco ATA continuously monitors its Ethernet connection to the switch or hub. If this connection is broken, the Cisco ATA starts an internal timer that runs until a configurable timeout period expires. Once the timeout value is reached, the Cisco ATA automatically reboots. This timeout value is configured by using the FeatureTimer2 configuration parameter. For more information, see the "FeatureTimer2" section on page 5-39.

Diagnostics for Debugging

You can use the following parameters to troubleshoot operation issues:

- NPrintf, page 5-73—Specify the IP address and port where debug information is sent.
- TraceFlags, page 5-73—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 Parameters

- DialPlan, page 5-64
- DialPlanEx, page 5-72

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 5-45—Bit 7

Display-Name Support for Caller ID

For caller ID purposes, you can configure a name to correspond to the phone number of the Cisco ATA input ports. This name will be displayed at the remote endpoint when a call originates from this Cisco ATA.

Related Parameters

- DisplayName0, page 5-29—for the **Phone 1** port
- DisplayName1, page 5-29—for the **Phone 2** port

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 5-13
- AltGk, page 5-14

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 5-9—Enter the LAN IP address of the NAT through which the Cisco ATA will communicate.
- NATIP, page 5-21—Enter the WAN IP address of the NAT through which all external SIP user agents will communicate.
- SIPPort, page 5-19—Enter a new port for SIP messages (optional).
- MediaPort, page 5-30—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 5-22—Bits 0 to 11 are for specifying the retransmission period.
- NatServer, page 5-22—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 5-48—Use for time-stamping incoming calls (offset from Greenwich Mean Time) with local time.
- NTPIP, page 5-11—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 5-12—Use to configure an alternate NTP server IP address.
- ConnectMode, page 5-41—Used to control the connection mode of the SIP protocol.

Obtaining Network Status Before and After Getting IP Connectivity

Using voice configuration menu code **3123#,** you can obtain basic network status to use for diagnostic purposes prior to getting IP connectivity. For detailed information, see the "Obtaining Network Status Prior to Getting IP Connectivity" section on page 9-11.

Use the Cisco ATA Stats Web page `(http://<Cisco ATA IP address>/stats)` to display network status information after obtaining IP connectivity. For detailed information, see the "Obtaining Network Status After Getting IP Connectivity" section on page 9-12.

Privacy Options

The privacy options described in this section provide users with stricter control over the appearance of their caller line identification at the SIP message level. These options not only protect the user's anonymity at the caller site but also prevent network-level sniffer-type applications from gaining access to restricted information that is in transit.

This section contains the following topics:

Network Infrastructure Requirements

For user privacy to work effectively on the Cisco ATA, the proxy or proxies deployed in the IP network must be capable of the following:

- Privacy token support.
- Determining whether a third party involved in a diversion case is *trusted* so that the proxy can forward private Diversion headers to that site.
- Determing that a site is not *trusted* and being able to change the user names to *Anonymous* in Diversion headers before including these headers in resulting INVITE requests.

Gateways deployed in the IP Network must be capable of the following:

- Privacy token support
- Redirecting a number by correctly setting the presentation bits in the Redirecting Number field of the Initial Address Message (IAM) message, based on the level of privacy requested in the Diversion header.

Anonymity for Called Party

The Cisco ATA provides an option to use the *Anonymous* user name in the TO header in all outgoing SIP INVITE requests when the Cisco ATA is the calling party.

To enable this option, set bit 30 of the Cisco ATA ConnectMode parameter to 1. For more information, see the "ConnectMode" section on page 5-41.

This feature guarantees the anonymity of the called party (in the To header) on every call that the Cisco ATA initiates. However, the main intent of this feature is to hide the identity of the called party in the event that the call is diverted to a not-trusted address and caller-ID-restricted is configured on the diverting Cisco ATA. In this case, the proxy has the responsibility of removing user-sensitive data before the call is sent to the not-trusted address.

The Cisco ATA handles the TO header because proxies are not allowed to change the TO header.

Anonymous User Name Support for SIP INVITE Requests

The Cisco ATA provides an option to use the *Anonymous* user name in the FROM and CONTACT headers and in the *o=* line *(*also called th*e origin* line*)* of the Session Description Protocol (SDP) header in SIP INVITE requests to the far end. The *Anonymous* user name is used when the following three conditions are met:

- The Cisco ATA is acting as the caller.
- The Cisco ATA Caller Line Identification Restriction (CLIR) feature is enabled, which can be performed in one of two ways:
  - By setting bit 3 of both the CallFeatures and PaidFeatures parameters to 0. (For the **Phone2** port of the Cisco ATA, you would set bit 19 to 0 for each parameter.) For more information on these parameters, see the "CallFeatures" section on page 5-35 and the "PaidFeatures" section on page 5-36.
  - By enabling the CLIR on a per-call basis by using the call command dial string. Enabling the CLIR on a per-call basis requires that the dial string sequence (typically ***69**) that users enter on their dialpad prior to dialing the phone number match the specified CLIR string defined in the call command. For more information, see Chapter 6, "Call Commands."

- Bit 27 of the Cisco ATA ConnectMode parameter is set to 1. For more information, see the "ConnectMode" section on page 5-41.

Example Cisco ATA INVITE Messages

The following example SIP INVITE messages show how the *Anonymous* user name would appear in the context of these messages:

```
INVITE sip:9401@192.168.2.146:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 192.168.2.96:5060;branch=7cca152b-232af34f-3f0b0c31-3cea3a52-1
Via: SIP/2.0/UDP 192.168.3.117:5060;received=192.168.3.117
Supported: timer
From: "Anonymous" <sip:Anonymous@192.168.2.96;user=phone>;tag=173234376
To: <sip:9401@192.168.2.96;user=phone>
Call-ID: 1157628352@192.168.3.117
CSeq: 1 INVITE
Contact: "Anonymous" <sip:Anonymous@192.168.3.117:5060;user=phone;transport=udp>
User-Agent: Cisco ATA 186  v3.0.0 atasip (030619A)
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER
Expires: 300
Content-Length: 252
Content-Type: application/sdp
v=0
o=Anonymous 6269 6269 IN IP4 192.168.3.117
```

Privacy Token Support for SIP Diversion Header

Proxies typically use the privacy token value contained in the Diversion header of SIP INVITE messages and 3xx Redirection responses to determine whether any of the diverting party's user names should be changed before forwarding the message to untrusted addresses.

This feature applies only when the following two conditions are met:

- The Cisco ATA is the callee and is forwarding or diverting a call.
- Bit 27 of the ConnectMode parameter is set to 1. For more information, see the "ConnectMode" section on page 5-41.

Before forwarding the call, the Cisco ATA appends a *privacy=[full\off]* field to the end of the Diversion header in a *302 Moved Temporarily* message.

The value of the *privacy=[full\off]* field depends on the setting of bit 3 of the CallFeatures and PaidFeatures parameters. (Bit 19 is the applicable bit for the **Phone2** port of the Cisco ATA.) This bit is for configuring either the Caller Line Identification Restriction (CLIR) or Caller Line Identification Presentation (CLIP) feature.

- If CLIR is the configured feature, then *privacy=full* is appended to the Diversion header.
- If CLIP is the configured feature, then *privacy=off* is appended to the Diversion header.

For more information on CLIR and CLIP, see the "CallFeatures" section on page 5-35 and the "PaidFeatures" section on page 5-36.

Progress Tones

Values for the following parameters (all defined in the "Tone Configuration Parameters" section on page 5-53) must be determined based on the country in which the Cisco ATA is located:

- DialTone
- BusyTone
- ReorderTone
- RingBackTone
- CallWaitTone
- AltertTone

Real-Time Transport Protocol (RTP) Statistics Reporting

To monitor the quality of service for the media stream, you can access RTP packet statistics of the two voice ports and their channels by opening the following page on the Cisco ATA Web server:

```
<Cisco ATA IP address>/rtps
```

For detailed information about RTP statistics reporting, see the "Real-Time Transport Protocol (RTP) Statistics Reporting" section on page 9-13.

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 5-41—Bit 22

Redundant Proxy Support for BYE/CANCEL Request

The Cisco ATA retries a BYE or CANCEL request using an alternate SIP proxy if the GkOrProxy parameter value is configured with a domain name. The BYE request requires special consideration because the destination can be either the SIP endpoint client or proxy server.

For a SIP user agent client, if a SIP proxy server does not include a Record-Route header in its *200 OK* response to an INVITE request, the destination of a BYE request is the SIP URL specified in the Contact header of the response. This URL is usually an IP address; therefore, redundancy is not possible.

For a SIP user agent server, if a SIP proxy server does not include a Record-Route header in the original INVITE request, the destination of a BYE request is the SIP URL specified in the Contact header of the request. This URL is also usually an IP address; therefore, redundancy is not possible.

If a Record-Route header is present in the SIP proxy server *200 OK* response to an INVITE request or in an original INVITE request, the BYE request is sent to the first SIP URL specified in the Record-Route header. If the SIP URL is a proxy domain name, then proxy redundancy is possible. Therefore, for SIP proxy redundancy to work for a BYE request, the RequestURL must be a domain name.

Related Parameter

GkOrProxy, page 5-13

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 5-38—Bits 0 to 3 control the maximum time the Cisco ATA redials a number.
- FeatureTimer, page 5-38—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 5-37—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.”

Retransmitting SIP requests and SIP Responses

You can configure the number of Cisco ATA transmission attempts for some SIP requests and responses to requests from the SIP user agent. For details on which requests and responses are configurable, see the "MsgRetryLimits" section on page 5-24.

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 exepcts the usual 100/180/200 responses from the user agent.

This section contains the following topics:

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: `http://<Cisco_ATA_IP_address>/dev`

where Cisco_ATA_IP_address 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:

- GkOrProxy, page 5-13—Set to the value of 0 (zero).
- UID0, page 5-15—Set to the unique telephone number of the **Phone 1** port of the Cisco ATA.
- UID1, page 5-16—Set to the unique telephone number of the **Phone 2** port of the Cisco ATA.
- SIPRegOn, page 5-20—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#**

SipOutBoundProxy Support

If the SipOutBoundProxy 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 SipOutBoundProxy 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 SipOutBoundProxy is enabled, the Cisco ATA determines whether to retry to connect with the backup SipOutBoundProxy 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

- SipOutBoundProxy, page 5-21
- AltGkTimeOut, page 5-15

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 5-13
- AltGk, page 5-14
- AltGkTimeOut, page 5-15

SIP Session-Timer Support

The SIP Session Timer is a keepalive mechanism for a SIP session, and is used to determine whether a call is still active when one of the following conditions occurs:

- The user agent fails to send a BYE message to the Cisco ATA at the end of a SIP session.
- The BYE message that the user agent sends to the Cisco ATA is lost because of network problems.

To avoid a a situation where a user agent waits indefinitely for a BYE message, the user agent sends periodic re-INVITE requests (or session refresh requests) to the Cisco ATA to keep the session alive. The interval betwen these session-refresh requests is negotiated with the use of Session-Expires/Min-SE headers and 422 (*Session Interval Too Small*) messages. If the Cisco ATA does not receive a session-refresh request before the negotiated interval expires, the session is considered terminated. Both user agents then send BYE messages and disconnect the session.

The Cisco ATA supports session timing only when both the caller and callee support this feature. Also, the Cisco ATA does not support the UPDATE method; therefore, all session-refresh requests are performed by means of the re-INVITE method.

Note The Cisco ATA implementation of the SIP Session Timer is based on the document *draft-ietf-sip-session-timer-11.txt*, which can be found on the Internet.

Related Parameters

The following three parameters are used to configure SIP session timing:

- SessionTimer, page 5-26—Example settings are included and described.
- SessionInterval, page 5-28
- MinSessionInterval, page 5-28

Status of Phone Service Using HTTP

You can use the following command to provide the status of various call features:

```
http://ipaddress/service/
```

where *ipaddress* is the IP address of the Cisco ATA whose status you are checking.

The Web page invoked from this command provides information about the following features:

- CWait (call waiting)—The status is shown as either *on* or *off*.
- CFwdU (call forwarding unconditional)
- CFwdNA (call forwarding no answer)
- CFwdB (call forward busy)
- CRtn (call return number)

For all features except call waiting, the information on the Web page either provides the applicable phone number, which also means that the feature has been activated, or *N/A* is shown if the feature has not been activated.

STUN Support

The Cisco ATA supports a Simple Traversal of UDP through NAT (STUN) client, as described in *RFC 3489*. The Cisco ATA obtains the IP address and port mappings of the NAT and uses them accordingly in a SIP message.

This section contains the following topics:

Types of NATs

Four types of NATs can be used:

- Full Cone NAT—This type of NAT maps all requests from the same internal IP address and port to the same external IP address and port. Any external host can send a packet to the internal host only if the internal host had previously sent a packet through the NAT.
- Restricted Cone NAT—This type of NAT maps all requests from the same internal IP address and port to the same external IP address and port. An external host (with IP address *X*) can send a packet to the internal host only if the internal host had previously sent a packet to IP address *X*.
- Port Restricted Cone NAT—This type of NAT maps all requests from the same internal IP address and port to the same external IP address and port. An external host (with IP address *X* and source port *P*) can send a packet to the internal host only if the internal host had previously sent a packet to IP address *X* and port *P*.
- Symmetric NAT—In a symmetric NAT, all requests from the same internal IP address and port to a specific destination IP address and port are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

A STUN server can help facilitate traversing through most NATs, except for symmetric NATs.

NAT Traversal

To help facilitate traversal through a NAT, the Cisco ATA uses the same signaling port for transmitting and receiving SIP messages and the same media port for transmitting and receiving media. Before an external host can send a packet to the Cisco ATA behind a NAT, the Cisco ATA must already have sent a packet through the NAT.

An external host can communicate with a Cisco ATA behind a full cone NAT by sending packets to the mapped port. If the Cisco ATA is behind a restricted cone NAT, an external host would have to send packets from the same IP address that it used to receive packets from the Cisco ATA.

If the Cisco ATA is behind a port-restricted cone NAT, an external host would have to send packets from the same IP address and port it used to receive packets from the Cisco ATA. Because a symmetric NAT creates different mapping for every packet with a different destination IP address and/or port, the Cisco ATA cannot traverse through this type of NAT.

If properly configured, the Cisco ATA on power up contacts the specified STUN server to obtain the IP address and port mappings of the NAT before registering with the registration server. The Cisco ATA substitutes this mapping information into the Via and Contact headers. Each time the Cisco ATA sends an INVITE message, the Cisco ATA obtains IP address and port mappings from the STUN server and substitutes this mapping information into the Via, Contact, and SDP *c*= and *m*= headers. This allows the SIP proxy server and remote user agents to to communicate with the Cisco ATA through most NATs.

STUN Configuration Parameters

Two parameters control the operation of the Cisco ATA with a STUN server:

- NatTimer—This parameter allows the following configuration:
  - Interval of keep-alive packets
  - STUN mode to use
  - Destination of keep-alive packets

  For more information, see the "NatTimer" section on page 5-22.
- NatServer—This parameter is used to specify a server to which keep-alive packets are sent. If the NatServer is a STUN server and STUN mode is selected, the Cisco ATA obtains IP address and port mapping information from this server.

  For more information, see the "NatServer" section on page 5-22.

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.

Toll Restrictions for Call Forwarding and Outgoing Calls

You can configure the Cisco ATA to block certain numbers from call forwarding and to display certain numbers for caller ID.

Related Dial Plan Rules

- 'F' Rule for Call Forwarding Blocking, page 5-69
- 'D' Rule for Displaying Caller ID, page 5-70

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 5-41—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 5-40—Bits 20 to 25

Voice Prompt Confirmation for Call Waiting and Call Forwarding

You can configure the Cisco ATA to automatically call a voice announcement server whenever the status of call-waiting or call-forwarding services changes. The telephone number of the server to which the Cisco ATA will send an INVITE request is specified by a configurable base number and several pre-assigned extension numbers. The extension numbers correspond to the service and the state change of the service.

You must configure the following information:

- Base Number, page 4-21
- Relevant Bit of OpFlags Parameter, page 4-21

Base Number

The base number is the first part of a number that the Cisco ATA calls, as specified in the dial plan using rule ‘B.’ To set this base number using rule plan ‘B’, you would use ‘B’ followed by the desired base number. If, for example, the desired base number is 1234, you would add the rule ‘B1234’ to your dial plan.

Note Each dial plan rule must be partitioned from other rules with a vertical bar (|).

The telephone number that the Cisco ATA will call will always consist of the base number followed by a two-digit extension. The extensions corresponding to the service type and service transition, as shown below. These extensions are not configurable. If the administrator has configured a base number of 1234 and call forward on busy is enabled, the called number is 123403.

Cisco ATA Service/Transition Extensions

- Call Waiting Enable—Extension 00
- Call Waiting Disabled—Extension 01
- Call Forward All Enabled—Extension 02
- Call Forward All Disabled—Extension 05
- Call Forward Busy Enabled—Extension 03
- Call Forward Busy Disabled—Extension 05
- Call Forward No Answer Enabled—Extension 04
- Call Forward No Answer Disabled—Extension 05

Relevant Bit of OpFlags Parameter

The relevant OpFlags parameter bit is determined by the service that is enabled or disabled, and the identity of the transition. The service types that will prompt a call to the announcement server are call waiting and call forward. Both of these services can undergo an *enable* transition or a *disable* transition. For the Cisco ATA to call the server, the applicable OpFlags bit must be set. Table 4-3 provides a mapping of each relevant OpFlags bit to its corresponding service/transition state or states.

Table 4-3 Service/Transition and Corresponding OpFlags Bit

Service/Transition	OpFlags Bit
Call Waiting Enabled	Bit 18 (mask = 0x40000)
Call Waiting Disabled	Bit 19 (mask = 0x80000)
Call Forward All Enabled	Bit 16 (mask = 0x10000)
Call Forward All Disabled	Bit 17 (mask = 0x20000)
Call Forward Busy Enabled	Bit 16 (mask = 0x10000)
Call Forward Busy Disabled	Bit 17 (mask = 0x20000)
Call Forward No Answer Enabled	Bit 16 (mask = 0x10000)
Call Forward No Answer Disabled	Bit 17 (mask = 0x20000)

XML Pages of Cisco ATA Information

The Cisco ATA provides XML pages that contain the following Cisco ATA information:

Current configuration

To obtain the XML configuration page, issue the following command:

```
http://ipaddress/dev.xml
```

where *ipaddress* is the IP address of the Cisco ATA whose configuration you wish to access.

This XML page is only for retrieving the configuration of a Cisco ATA; you cannot change configuration values on this page.

This XML page is password protected. You can enter the password by means of your Web browser, or you can issue the following command:

```
curl -d "ChangeUIPasswd=<passwd>&ChangeUIPasswd=&ChangeUIPasswd=
       &apply=apply"<ip addr>/dev.xml
```

where <*passwd*> is the Cisco ATA password and <*ip addr*> is the IP address of the Cisco ATA.

Current statistics

To obtain this statistics page, issue the following command:

```
http://ipaddress/stats.xml
```

where *ipaddress* is the IP address of the Cisco ATA whose statistics you wish to access.

This XML page is password protected. You can enter the password by means of your Web browser, or you can issue the following command:

```
curl -d "ChangeUIPasswd=<passwd>&ChangeUIPasswd=&ChangeUIPasswd=
       &apply=apply"<ip addr>/stats.xml
```

where <*passwd*> is the Cisco ATA password and <*ip addr*> is the IP address of the Cisco ATA.

Current service values

To obtain this service page, issue the following command:

```
http://ipaddress/service.xml
```

where *ipaddress* is the IP address of the Cisco ATA whose service values you wish to access.

This XML page is password protected. You can enter the password by means of your Web browser, or you can issue the following command:

```
curl -d "ChangeUIPasswd=<passwd>&ChangeUIPasswd=&ChangeUIPasswd=
       &apply=apply"<ip addr>/service.xml
```

where <*passwd*> is the Cisco ATA password and <*ip addr*> is the IP address of the Cisco ATA.

Complete Reference Table of all Cisco ATA SIP Services

Table 4-4 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 4-4 Configurable Features and Related Parameters

Configurable Feature	Related Parameter
802.1Q packet tagging	VLANSetting, page 5-12
Anonymity for called third party	ConnectMode, page 5-41—Bit 30
Anonymous user name support	ConnectMode, page 5-41—Bit 27
Audio compression and decompression	LBRCodec, page 5-32
Audio level of FXS ports	FXSInputLevel, page 5-52, FXSOutputLevel, page 5-52
Backup proxy configuration	AltGk, page 5-14
Backup proxy timeout	AltGkTimeOut, page 5-15
Call forward enable/disable	ConnectMode, page 5-41—Bit 17
Call forwarding—Maximum times allowed	MAXRedirect, page 5-20
Call commands	CallCmd, page 5-37, Chapter 6, “Call Commands”
Call features	CallFeatures, page 5-35
Caller ID format	CallerIdMethod, page 5-49
Call waiting	SigTimer, page 5-40
Call-waiting call ring timeout	FeatureTimer, page 5-38
Call-waiting hang-up alert	ConnectMode, page 5-41—Bit 25
Call-waiting state specified	ConnectMode, page 5-41
Cisco Discovery Protocol	OpFlags, page 5-45
CNG tone detection	AudioMode, page 5-32
Configuration update interval	CfgInterval, page 5-6
Debugging and diagnostics	NPrintf, page 5-73, TraceFlags, page 5-73, SyslogIP, page 5-74, SyslogCtrl, page 5-75
Dial plan commands	DialPlan, page 5-64
Domain name server	DNS1IP, page 5-10
DNS hostname lookup	ConnectMode, page 5-41
DTMF method	AudioMode, page 5-32
Encryption	EncryptKey, page 5-6, EncryptKeyEx, page 5-7
Fax CED tone	AudioMode, page 5-32
Fax mode on a per-call basis	CallFeatures, page 5-35, PaidFeatures, page 5-36
Fax pass-through	AudioMode, page 5-32, ConnectMode, page 5-41

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

Configurable Feature	Related Parameter
G.711 codec	AudioMode, page 5-32
Hook flash	AudioMode, page 5-32, SigTimer, page 5-40
IDs for phone lines	UID0, page 5-15, UID1, page 5-16
IP audio and signaling packets—precedence and delay	TOS, page 5-34
IP-like address in dial plan	IPDialPlan, page 5-72
Login ID	LoginID0, page 5-17, LoginID1, page 5-18
Low bit-rate codec	LBRCodec, page 5-32
Mixing of tones	ConnectMode, page 5-41
Network Address Translation (NAT) server—Maintain during session	NatServer, page 5-22
NSE payload number	ConnectMode, page 5-41
NTP IP address	NATIP, page 5-21
On-hook delay	FeatureTimer, page 5-38
Outbound proxy	SipOutBoundProxy, page 5-21
Paid features	PaidFeatures, page 5-36
Passwords for phone lines	PWD0, page 5-16, PWD1, page 5-17
Polarity	Polarity, page 5-51
Polarity reversal before and after caller ID signal	CallerIdMethod, page 5-49
Privacy token support for SIP diversion header	ConnectMode, page 5-41—Bit 27
Received = tag enable/disable	ConnectMode, page 5-41
Receiving-audio codec preference	RxCodec, page 5-31
Redial time if line is busy	FeatureTimer, page 5-38
Refresh Cisco ATA using Web server	OpFlags, page 5-45
REGISTER messages	ConnectMode, page 5-41
Registration removal	ConnectMode, page 5-41
Reset Cisco ATA using Web server	OpFlags, page 5-45
Retransmission interval for NAT server	NatTimer, page 5-22
Retry interval if line is busy	FeatureTimer, page 5-38
Ringback tone—send to caller	ConnectMode, page 5-41
Ring-cadence pattern	RingOnOffTime, page 5-64
RTP media port	MediaPort, page 5-30
RTP packet size	NumTxFrames, page 5-34
RTP statistics	TraceFlags, page 5-73

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

Configurable Feature	Related Parameter
Secondary domain name server	DNS2IP, page 5-11
Silence suppression setting	AudioMode, page 5-32
SIP call return	ConnectMode, page 5-41
SIP proxy registrar address	GkOrProxy, page 5-13
SIP retransmission attempts for requests or responses	MsgRetryLimits, page 5-24
SIP proxy registration renewal	SIPRegInterval, page 5-19
SIP registration enable/disable	SIPRegOn, page 5-20
SIP-request listening port	SIPPort, page 5-19
SIP session-timer settings	SessionTimer, page 5-26, SessionInterval, page 5-28, MinSessionInterval, page 5-28
Static network router probe	OpFlags, page 5-45
STUN support	NatTimer, page 5-22, NatServer, page 5-22
TFTP file—not using internally generated name	OpFlags, page 5-45
Timing values	SigTimer, page 5-40, FeatureTimer, page 5-38, FeatureTimer2, page 5-39
Time zone offset	TimeZone, page 5-48
Tones: BusyTone, CallWaitTone AlertTone, DialTone, ReorderTone, and RingBackTone parameters	Tone Configuration Parameters, page 5-53
Tracing	TraceFlags, page 5-73
Transmitting-audio codec preference	TxCodec, page 5-31
VLAN encapsulation	OpFlags, page 5-45
VLAN mode	OpFlags, page 5-45
WAN address of NAT	NATIP, page 5-21
Web configuration—disallowing	OpFlags, page 5-45