Release Notes for the Cisco ATA 186 and Cisco ATA 188 Release 2.16.2

Sept. 19, 2003

These release notes describe newly incorporated features, changed features or changed behavior, resolved issues, and open issues for the Cisco ATA 186 and the Cisco ATA 188 for Release 2.16.2 (SIP and H.323 protocols).

Note These Release Notes also contain information from previous 2.16x releases.

Note The term *Cisco ATA* refers to both the Cisco ATA 186 and the Cisco ATA 188.

Contents

These release notes provide the following information:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction to the Cisco ATA Analog Telephone Adaptor

The Cisco ATA is an analog telephone adaptor that allows regular analog telephones to operate on IP-based telephony networks. The Cisco ATA supports two voice ports, each with its own independent telephone number.

Two Cisco ATA products are available to Cisco customers—the Cisco ATA 186 and the Cisco ATA 188. Both products run the same software and have two voice ports. The difference between these products is that the Cisco ATA 186 has one RJ45 port that provides access to an Ethernet network, while the Cisco ATA 188 has an Ethernet switch and two RJ45 ports. The Cisco ATA 188 has one RJ45 port for access to an Ethernet network and a second RJ45 port for connecting a downstream Ethernet device such as a PC.

Downloading and Upgrading the Software

Before you can use the Cisco ATA Release 2.16.2, you must first download and upgrade the Cisco ATA software. You can download the software, after logging in, at:

http://www.cisco.com/cgi-bin/tablebuild.pl/ata186

Note If you are using the Cisco ATA executable-file-upgrade method, check with the administrator of the TFTP server to make sure that the TFTP upgrade method is disabled. Otherwise, the Cisco ATA might downgrade to an old image via TFTP.

For more information about downloading and upgrading software, see the Cisco ATA administrator's guides for the signaling protocol you are using. The administrator's guides can be found at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/voice/ata/ataadmn/index.htm

New Features in Release 2.16

This section contains information on new features for Cisco ATA Release 2.16:

General Features

This section contains information on new features for Cisco ATA Release 2.16 for both SIP and H.323:

Local Tone Playout Reporting

The Cisco ATA inserts tone type IDs into its debug log.

To help analyze call flows, the tone locally played by the Cisco ATA to the FXS port is reported by means of the prserv debug log. Local tones are different from other tones because local tones are not carried within the inband audio. Instead, the Cisco ATA is prompted by a network event to play the tone, and the Cisco ATA generates the tone for the exclusive purpose of playing it to the attached telephone handset. For example, during a call between the Cisco ATA and a far-end phone, the far-end user might press a digit on the dial pad, thus sending an AVT Named Signaling Event to the Cisco ATA. This event prompts the Cisco ATA to generate a DTMF tone and to play the tone locally to the Cisco ATA phone.

Table 1 lists the tone type identifier and its description for local tone reporting.

Table 1 Tone Type Identifiers

Tone Type ID	Description
0	Dial tone
1	Busy tone
2	Reorder tone
3	Ringback tone
4	Call-waiting tone
5	Warning or confirmation tone
6	DTMF digit 0
7	DTMF digit 1
8	DTMF digit 2
9	DTMF digit 3
10	DTMF digit 4
11	DTMF digit 5
12	DTMF digit 6
13	DTMF digit 7
14	DTMF digit 8
15	DTMF digit 9
16	DTMF digit A
17	DTMF digit B
18	DTMF digit C
19	DTMF digit D
20	DTMF digit *
21	DTMF digit #
22	CPE alert signal (for off-hook Caller ID generation)

Table 1 Tone Type Identifiers (continued)

Tone Type ID	Description
23	Outside dial tone
24	Prompt tone
25	Beep tone

Note For information on the prserv debug tool, see the "Configuring and Debugging Fax Services" section in the Cisco ATA administrator's guides.

Real-Time Transfer 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
```

The following RTP packet statistics are reported:

- rxDuration—the number of seconds since the beginning of reception
- rxPktCnt—the total number of RTP packets received
- rxOctet—the total number of RTP payload octets received (not including RTP header)
- latePktCnt—the total number of late RTP packets received
- totalLostPktCnt—the total number of lost RTP packets received (not including late RTP packets)
- avgJitter—an estimate of statistical variance of the RTP packet inter-arrival time, measured in timestamp unit. (Calculation is based on the formula in RFC1889.)
- txDuration—the number of seconds since the beginning of transmission
- txPktCnt—the total number of RTP packets transmitted
- txOctet—the total number of RTP payload octets transmitted

Using the refresh feature on the RTP Statistics page, you can obtain updated, real-time RTP statistics during a call.

Resetting Cisco ATA counters

To reset the Cisco ATA counters, do the following:

- Click the [Refresh] link to refresh the current counter values.
- Click the [Line 0] link to reset line 0 counter values.
- Click the [Line 1] link to reset line 1 counter values.

Note Inactive lines will be indicated as such.

Using Voice Configuration Menu for Status Reporting Prior to Getting IP Connectivity

Using voice configuration menu code **3123#,** you can obtain basic network status to use for diagnostic purposes. After you enter this code, the Cisco ATA announces a message in the following format:

`e123.D.0xX`

where:

- D is the VLAN ID (this is a non-zero value if the Cisco ATA has entered a VLAN)
- 0xX is a bitmap value in hexadecimal format. The definition of each bit is shown in Table 2.

Table 2 Voice Configuration Menu Network Status Bitmap

Bit Number	Description
0	Cisco ATA sent CDP request
1	VLAN ID acquired via CDP
2	Cisco ATA sent DHCP request
3	DHCP server offered IP address
4	Cisco ATA obtained IP address from DHCP server
5	Cisco ATA web server is ready

Example

If the hexadecimal value provided by the voice configuration menu is 0x1d, the network status of the Cisco ATA is shown in Table 3.

Table 3 Voice Configuration Menu Example Network Status

Bit Number	Description	Boolean Value
0	Cisco ATA sent CDP request	True
1	VLAN ID acquired via CDP	False
2	Cisco ATA sent DHCP request	True
3	DHCP server offered IP address	True
4	Cisco ATA obtained IP address from DHCP server	True
5	Cisco ATA web server is ready	False

Using Web Configuration Page for Status Reporting After Getting IP Connectivity

The Cisco ATA Stats Web page (`http://<Cisco ATA IP address>/stats`)displays the following information:

- `VLAN ID: D0`
- `tftpFile: S`
- `NTP: D1,D2,D3`

- `tftp: 0xX`

  where:

  – D0 is the VLAN ID. It should be non-zero if the Cisco ATA has entered a VLAN.

  – S is the tftp filename, which can be either ata<macaddress> or the filename supplied by the DHCP server.

  – D1 is the local time on the Cisco ATA.

  – D2 is the last NTP contact time.

  – D3 is the last successful NTP contact time.

  D1, D2, D3 values are shown in number of seconds since 00:00:00 **UTC**, **1970**-01-01. If no NTP response has been received from the NTP server, the values of D1, D2, and D3 are 0.

  – 0xX is a bitmap value in hexadecimal format. The definition of each bit is shown in Table 4.

Table 4 Web Configuration Menu Network Status Bitmap

Bit Number	Description
0	Cisco ATA sent request for configuration file, ata<macaddress>, to TFTP server
1	Cisco ATA sent request for configuration file, atadefault.cfg, to TFTP server
4	Cisco ATA sent request for image file to TFTP server
5	Cisco ATA failed to upgrade to the downloaded image file
8	Configuration file is not found
9	Bad configuration file
10	Checksum error for configuration file,
11	Decode error for configuration file (encryption related)
12	Configuration file is processed successfully

Example

If the hexadecimal value provided by the web configuration menu is 0x1011, the network status of the Cisco ATA is shown in Table 5.

Table 5 Web Configuration Menu Example Network Status

Bit Number	Description	Boolean Value
0	Cisco ATA sent request for configuration file, ata<macaddress>, to TFTP server	True
1	Cisco ATA sent request for configuration file, atadefault.cfg, to TFTP server	False
4	Cisco ATA sent request for image file to TFTP server	True
5	Cisco ATA failed to upgrade to the downloaded image file	False
8	Configuration file is not found	False
9	Bad configuration file	False
10	Checksum error for configuration file	False

Table 5 Web Configuration Menu Example Network Status (continued)

Bit Number	Description	Boolean Value
11	Decode error for configuration file (encryption related)	False
12	Configuration file is processed successfully	True

Pipelined DNS Query

In this release, the Cisco ATA performs a DNS query by first sending its request to DNS server number 1. Then, if DNS server number 1 does not respond to this request within one second, the Cisco ATA sends the same request to DNS server number 2. The Cisco ATA accepts the first response from either of the DNS servers, thereby reducing the time the Cisco ATA requires for name resolution if DNS server number 1 is down or not responding.

New Bit for DNS Name Resolution

The OpFlags parameter now uses a control bit (Bit 13, mask 0x2000) to allow DNS name resolution using both statically configured DNS IP addresses (by means of configuration parameters DNS1IP and DNS2IP) and DHCP server-supplied DNS IP addresses. Therefore, the Cisco ATA can query as many as four DNS IP addresses in one DNS query.

New CDP Discovery Implementation

CDP Discovery behavior is implemented as follows:

- Sends 3 CDP Discovery packets at one-second intervals.
- Wait five seconds after sending packets, then selects the CDP response with the highest auxiliary VLAN ID.
- Processes CDP packets that have an 802.1Q tag.

Note CDP packets do not normally have an 802.1Q tag.

New Features for SIP

The following list contains new SIP-specific features in Cisco ATA Release 2.16:

- REFER Method Support

  The Cisco ATA now supports the SIP REFER method for call transfer. When the Cisco ATA initiates a call transfer, it sends a REFER request to the remote user agent. If the remote user agent does not support the method, a "501 Not Implemented" response should be returned to the Cisco ATA. The Cisco ATA then re-initiates the call transfer using the BYE/Also method.

- Configurable Call Return Ring Delay

  When the Cisco ATA sends a call to a PSTN phone number, the call goes through a PSTN gateway that is connected to the local telephone company’s network.

  The PSTN gateway usually responds with a "183 Session Progress" response, followed by a "200 OK" response when the called party answers.

When a PSTN gateway returns a "486 Busy Here" response after a "183 Session Progress" response, the callback-on-busy feature fails on the Cisco ATA. The ATA interprets a 183 response as the far end phone ringing and terminates the automatic retry when even though the far end may actually be busy.

You can configure FeatureTimer parameter bits 13-15 to specify the amount of time that the Cisco ATA waits for a "486 Busy Here" response after receiving a 183 response. This allows a short time period for a 486 response to arrive before the Cisco ATA assumes a successful connection and rings the phone.

FeatureTimer Bit Values

You can configure bits 13-15 to have the values of 0-8, where 0 (the default) means there is no delay before the Cisco ATA rings the phone, and values 1-7 represent the number of seconds for the ring delay.

- Configurable Call Waiting Ring Timeout

  When a call arrives for a Cisco ATA port that is in use and has call-waiting enabled, the Cisco ATA plays a call-waiting tone. If the incoming call is not answered within a specified period of time, the Cisco ATA can reject the call by returning a "486 Busy" response to the remote user agent.

  You can configure FeatureTimer parameter bits 16-18 to specify the ringing period for incoming call-waiting calls. Valid values for bits 16-18 are 0-7, where 0 (the default) means the call-waiting ring never times out, and values 1-7 represent the number of 10-second units before the call-waiting ring times out. For example, a configured value of 4 means that the timeout value is 40 seconds.

  This feature can be disabled by either using the default value 0 or setting bits 16-18 to a value greater than the standard timeout for an incoming call as specified in SigTimer parameter bits 14-19. When this feature is disabled, a "480 Temporarily Not Available" response is returned to the remote user agent when the standard ring times out.

- Password Protection for Factory Reset and Local Upgrade

  Factory reset and local upgrade using the voice configuration menu can now be protected with the UI password. If the UI password (UIPassword parameter) is enabled, the Cisco ATA prompts the user for the password before a factory reset or upgrade is allowed.

  Note Users *must* keep the password in a safe location. If the UI password is lost or forgotten, there is no way to recover it.

  Use OpFlags parameter bits 28-31 to indicate whether factory reset and local upgrade options with the voice configuration menu are protected with the UI password.

OpFlags Configuration

To password-protect factory reset and local upgrade as previously described, you *must* configure OpFlags bits 28-31 with a value of **6**, and the UIPassword parameter must be enabled.

Any value other than **6** for these bits means that this feature is disabled and the Cisco ATA will not prompt the user for the UIPassword.

The default value is **0**.

New Features for H.323

There are no new H.323-specific features for Cisco ATA Release 2.16.

Changes in Release 2.16 for SIP and H.323

This section contains information on changed features for Release 2.16. for both the SIP and H.323 protocols:

- Support separate Type of Service (TOS) values for audio and signaling packets. The UDPTOS parameter has been renamed to TOS. With the TOS parameter, you can specify separate TOS bits for signaling and audio packets, as follows:
  - Bits 7-0 of TOS specify the TOS bit value of the audio packets.

    If Bits 7-0 are 0, the TOS bit value for audio packets defaults to 0xB8.
  - Bits 15-8 of TOS specify the TOS bit value of the signaling packets.

    If Bits 15-8 are 0, the TOS bit value for signaling packets defaults to 0x68.
  - Other bits are reserved and undefined at this time.

Note The previous value of the UDPTOS parameter is carried forward to the TOS parameter during a Cisco ATA upgrade.

- The VLANSetting parameter now allows you to specify different Class of Service (COS) bit values in the VLAN tag for audio and signaling packets. This is different from the previous Cisco ATA implementation, in which the VLANSetting parameter allowed you to specify separate COS bit values in the VLAN tag for UDP and TCP packets.
- The name of the sample configuration file that comes with the Cisco ATA software has changed for both SIP and H.323. In previous releases, the name of the sample file was example_uprofile.txt for both SIP and H.323.

  In Release 2.16.1, the name of the SIP sample configuration file is *sip_example.txt*; the name of the H.323 sample configuration file is *h323_example.txt*.
- The Cisco ATA no longer needs to reboot after a change to the TraceFlags parameter (currently used only for SIP). The configuration change will take effect immediately.

Changes in Release 2.16.1 for SIP only

The way in which the Cisco ATA removes a registration, determined by Bit 16 of the Cisco ATA parameter ConnectMode, has changed in Release 2.16.1.

Behavior Prior to Release 2.16.1 When this Bit is Set to 1

The Cisco ATA unregisters all existing registrations with the **Contact:*** SIP header and the **Expires:0** SIP header (or SIP URL) on power up and in all subsequent registration cycles prior to registering.

Behavior in Release 2.16.1 When this Bit is Set to 1

The Cisco ATA unregisters all registrations with **Contact:*** and **Expires:0** only on power up.

On subsequent registration cycles, the latest registration is removed with **Contact:<*SIP_URL*>;expires=0** prior to re-registering.

Changes in Release 2.16.2 for SIP and H.323

This section contains the following related topics, new for release 2.16.2:

- EncryptKeyEx Parameter, page 10
- New cfgfmt Tool, page 13

EncryptKeyEx Parameter

A new configuration parameter for Cisco ATA release 2.16.2, *EncryptKeyEx*, provides a stronger configuration file encryption key than the previously used *EncryptKey* parameter.

Syntax

`EncryptKeyEx:`*`rc4KeyInHex_n/macInHex_12`*

where:

- *rc4KeyInHex_n* is a hexadecimal string of one to 64 characters.
- /*macInHex_12* is the optional extension consisting of a forward slash (/) followed by the six-byte MAC address of the Cisco ATA to which the configuration file will be downloaded.

Description

Because the format of the EncryptKeyEx parameter is incompatible with the format of the *EncryptKey* parameter, a different configuration file is needed for the newer, EncryptKeyEx parameter. When the EncryptKeyEx parameter is set to 0, the Cisco ATA TFTP configuration file name is ata<MACaddress>. For example, if the Cisco ATA has a MAC address of 102030405060, the TFTP configuration file name is ata102030405060, or the value specified in the DHCP bootfile option field if that value is provided. When the value of EncryptKeyEx is 0, the value of EncryptKey (if nonzero) is used to encrypt the Cisco ATA configuration file.

If the EncryptKeyEx parameter is set to a nonzero value, the configuration file name is ata<MACaddress>.x and the value of the EncryptKeyEx parameter is used to encrypt the Cisco ATA configuration file.

Tool Required

You must use version 2.2 of the *cfgfmt* configuration-file generation tool to use the new EncryptKeyEx parameter. This tools comes bundled with Cisco ATA software version 2.16.2. This tool creates two configuration files—one file with the ata<MAC address> format, as the previous cfgfmt tool created, and one with the *.x* extension.

Refer to the "New cfgfmt Tool" section on page 13 for *cfgfmt* usage with the EncryptKeyEx parameter.

You can configure the EncryptKeyEx parameter by using the Cisco ATA Web configuration page or by using the TFTP configuration method. The following two examples both use the TFTP configuration method to illustrate how to use the EncryptKeyEx parameter.

Example 1

This example assumes the scenario in which a new Cisco ATA starts with a firmware version earlier than 2.16.2 and needs to upgrade to firmware version 2.16.2 to use the EncryptKeyEx parameter to encrypt its configuration file.

The Cisco ATA in this example has a MAC address of 102030405060.

Perform the following steps:

Step 1 Create a file called *ata102030405060.txt* by using the applicable *example.txt* file provided with the Cisco ATA software. (For example, for SIP, the example.txt file is called sip_example.txt.)

Step 2 Modify the *ata102030405060.txt* file with desired parameter values. The value of the EncryptKey parameter should be 0.

Step 3 Set the value of the EncryptKeyEx parameter to the chosen encryption key for ata<MACaddress>.x. In the EncryptKeyEx parameter specified in the configuration file, you can also restrict the EncryptKeyEx value to apply only to the Cisco ATA with a particular MAC address. For example, if the chosen key value is 231e2a7f10bd7fe, you can specify EncryptKeyEx as:

```
EncryptKeyEx:231e2a7f10bd7fe/102030405060
```

This means that only the Cisco ATA with the MAC address 102030405060 will be allowed to apply this EncryptKeyEx value to its internal configuration.

Step 4 Update the *upgradecode* parameter to instruct the Cisco ATA to upgrade to firmware version 2.16.2 by means of TFTP configuration. In this example, you would modify this parameter as follows:

```
upgradecode:3,0x301,0x400,0x200,0,69,0x030909a,ata18x-v2-16-2-030909a.zup
```

Step 5 Run the *cfgfmt* tool as follows:

```
cfgfmt -g ata102030405060.txt ata102030405060
```

This will generate the following two files:

- ata102030405060
- ata102030405060.x

ata102030405060 is unencrypted.

Note Some parameters, specified in the ptag.dat file used by the *cfgfmt* tool, are marked as sensitive information (these parameters could include UIPassword, UID, PWD0). These parameters are not included in the *ata102030405060* file if the *-g switch* is specified in the cfgfmt syntax. For more information, see the "New cfgfmt Tool" section on page 13.

ata102030405060.x is encrypted with EncryptKeyEx value.

Step 6 Place these two files on the TFTP server that the Cisco ATA will contact for its configuration files.

When the ATA is powered up, it will obtain its IP address from the DHCP server. If the DHCP server specifies the TFTP server address, the Cisco ATA will contact the TFTP server obtained from DHCP because the Cisco ATA is not preconfigured with a TFTP server address. The boot process is as follows:

a. The Cisco ATA downloads the configuration file ata102030405060 from the TFTP server.

b. The Cisco ATA applies parameter values in the file *ata102030405060* to its internal configuration while ignoring the EncryptKeyEx parameter (because the older version of the Cisco ATA does not yet recognize the EncryptKeyEx parameter).

c. The Cisco ATA upgrades to the 2.16.2 firmware load.

d. The Cisco ATA reboots.

e. The Cisco ATA downloads the configuration file *ata102030405060*.

f. The Cisco ATA applies the value of the EncryptKeyEx parameter to its internal configuration.

g. The Cisco ATA reboots.

h. The Cisco ATA EncryptKeyEx value is provisioned, so from this point forward the Cisco ATA will download the *ata102030405060.x* file at each reboot and each time the value configured in the *CfgInterval* parameter expires.

Note Although *EncryptKeyEx* is encrypted in the ata<MACaddress> file, and ata<mac> file does not contain other sensitive information, Cisco recommends that for absolute security you pre-provision the Cisco ATA as described in this example for a private network. Alternatively, you should remove ata<MACaddress> once *EncryptKeyEx* is provisioned.

Example 2

This example assumes a scenario in which a new Cisco ATA is already deployed (with the *EncryptKey* value set) with firmware version earlier than 2.16.2. The Cisco ATA needs to be upgraded to version 2.16.2 firmware to use *EncryptKeyEx* to encrypt its configuration file.

In this scenario, you would follow the same procedure as in Example 1, except that you need to set the *EncryptKey* value to the previously provisioned *EncryptKey* value. The difference is that the ata<MACaddress> file is now encrypted with *EncryptKey* because the Cisco ATA expects the ata<MACaddress> file to be encrypted with *EncryptKey.* This is the case so that the Cisco ATA can begin using the ata<MACaddress>.x file encrypted with En*cryptKeyEx*.

New cfgfmt Tool

Version 2.2 of the *cfgfmt* tool, which generates the Cisco ATA configuration file, supports a stronger encryption method. This version is compatible with older versions of the cfgfmt tool. When invoked on its own with no arguments, *cfgfmt* prints the following usage information:

```
cfgfmt version 2.2
usage: cfgfmt [options] input output

options:
-eRc4Passwd -- use Rc4Passwd to encrypt or decrypt input
-E -- do not use EncryptKey parameter's value in the input text file to encrypt the output
binary file
-xRc4Passwd -- use stronger Rc4Passwd to encrypt or decrypt input,RC4Passwd entered must
be in hex
-tPtagFile -- specify an alternate PtagFile path
-sip -- limit to sip protocol parameters
-h323 -- limit to h323 protocol parameters
-mgcp -- limit to mgcp procotol parameters
-sccp -- limit to sccp protocol parameters
-g -- omit sensitive parameters in old ata<mac> file
```

The *cfgfmt* tool, version 2.2, also combines all parameter descriptions of all protocols into a single ptag.dat file. If you want to include only a particular protocol configuration parameter in the output profile, you need to specify one of the four protocol switches: -sccp, -mgcp, -h323, and -sip, as in the following example:

```
cfgfmt -sip ata000102030405.txt ata000102030405
```

The -xRC4Password switch is mainly useful for decrypting the ".x" suffix profile, as shown below:

```
cfgfmt -sip -x0ab52123476231233a3 ata000102030405.x
```

This means to treat ata00102030405.x as the binary profile encrypted with the stronger encryption key "0ab52123476231233a3", then decrypt the file and display its textual content. This is useful only for debugging purposes to check the content of a binary profile.

The *-g* switch is used to exclude sensitive information from the non ".x" suffix profile (the old ata<mac> formatted profile). This is useful for provisioning the stronger EncryptKeyEx parameter using the old ata<MACaddress> formatted profile while keeping sensitive information from being available from the old ata<MACaddress> file. The ptag.dat file controls sensitive information.

Resolved Issues in Cisco ATA Release 2.16.2

This section lists the issues in previous releases of the Cisco ATA that are resolved in Release 2.16.2 or in prior 2.16x releases:

Resolved SIP Issues

This section lists the issues in previous releases of the Cisco ATA that are resolved in Cisco ATA Release 2.16 and later for SIP only:

Release 2.16

- CSCdz03610

  Out-of-band DTMF does not always work between the Cisco ATA and Cisco IOS-based gateways.

- CSCdz23724

  Ringing of the telephone handset may be delayed if the Cisco ATA performs a DNS query on the From header to prepare for the local call-return feature.

- CSCdz49720

  When the combined length of record-route uniform resource identifiers (URIs) and contact-header URIs is more than 318 bytes, Cisco ATA behavior is abnormal.

- CSCdz50247

  The Cisco ATA does not always send an acknowledgment (ACK) message after receiving a SIP proxy *5xx* response to an INVITE message.

- CSCdz61384

  A configurable option is needed for the Cisco ATA to include or exclude the port in a *Refer-To* header.

- CSCdz74453

  The Cisco ATA does not parse the IP address in the SIP *received=<ip-addr>* parameter if the *rport=<port>* parameter directly follows the *received=* parameter.

- CSCdz74468

  Configuring two DNS “A” records with the same domain name for the primary and secondary SIP proxy servers can cause problems for the Cisco ATA.

- CSCdz74514

When the gateway returns a *486* response to the Cisco ATA following a *183* response, the Cisco ATA callback-on-busy feature fails.

- CSCdz82086

  Out-of-band DTMF data packets are sent with fixed duration and an incremental timestamp instead of a fixed timestamp and incremental duration. This can cause a remote media server to detect only the first digit in a series of digits.

- CSCdz87773

  If the Cisco ATA sends an INVITE message that includes the *user=phone* parameter, the corresponding ACK message does not always contain the *user=phone* parameter.

- CSCdz89882

  The Cisco ATA does not process the *Expires* parameter from the SIP proxy server.

- CSCea05656

  Sweden CallWaitTone does not play two beeps.

- CSCea05692

  The call-waiting tone cannot be played only one time.

- CSCea13176

  When the Contact header in the *200 OK* response from the SIP proxy does not contain a User ID, the Route header in the Cisco ATA ACK message contains the Contact IP address with an empty User ID field.

- CSCea26155

  The PROTOS test-suite for SIP can cause the Cisco ATA to operate improperly, such as rebooting or hanging. Cisco recommends that customers with earlier software versions upgrade to this latest release.

Release 2.16 Build 030509a

- CSCea69889

  The Cisco ATA Telephony Adapters running SIP are incorrectly building a "302 Moved Temporarily" message. When the Cisco ATA receives a NOTIFY message during an existing call flow, the Cisco ATA uses the session information from the NOTIFY instead of the original INVITE or 180 RINGING message.

- CSCea79418

  Each time after a call is placed or received, subsequent Cisco ATA REGISTER requests have the same Call-ID but a different From tag. The From tag should remain the same in subsequent registrations.

- CSCea93969

  Cisco ATAs that are configured to handle G.723 calls sometimes experience lost audio when an incoming call-waiting call arrives.

- CSCeb01064

  The value of the From header in a SIP invite message changes after eight minutes of operation.

- CSCeb01252

  The Cisco ATA, when acting as the callee, does not provide SIP-requested credentials. Instead, the Cisco ATA increments the CSeq counter and resubmits the request without providing credentials.

- CSCeb01287

  The Cisco ATA incorrectly sends an ACK message that contains credentials to the SIP proxy even when the INVITE message did not contain credentials.

- CSCeb11582

  The Cisco ATA does not retry the DNS SRV query after a failure.

- CSCeb11817

  The Cisco ATA does not fail over to a second IP address returned by a DNS query.

Release 2.16.1

- CSCea42480

  The Cisco ATA ignores the *Require:100rel* header and processes call.

- CSCea69889

  The Cisco ATA builds a *302 Moved Temporarily* message incorrectly after receiving a NOTIFY message.

- CSCea93969

  The Cisco ATA loses G.723 audio when call waiting occurs.

- CSCeb01064

  The Cisco ATA *From* header domain value changes SRV record name.

- CSCeb17953

  The Cisco ATA stops the registration process if it receives an unexpected response to a REGISTER request.

- CSCeb19228

  The callback-on-busy feature does not work for calls to a PSTN.

- CSCeb23060

  Upon receiving a *4xx* response to a REGISTER request from a backup proxy, the Cisco ATA needs to continue retrying the request with the primary proxy.

- CSCeb24556

  The Cisco ATA may fail to send a ring tone when acting as a transfer target in a blind transfer.

- CSCeb28218

  The Cisco ATA, while in a call, detects audio from an incoming call.

- CSCeb32210

  When the SDP attribute *a=fmtp* appears before the attribute *a=rtpmap*, the Cisco ATA will not send out-of-band DTMF digits.

- CSCeb35955

  Attended call transfers occur even when this feature is disabled via the PaidFeature configuration parameter.

- CSCeb36752

  Call forwarding does not work when the Cisco ATA detects a busy signal.

- CSCeb37037

  The Cisco ATA stops registering after a 2.16 upgrade is performed.

- CSCeb37043

  The call-waiting default user setting cannot be controlled by the CallFeatures configuration parameter when the Cisco ATA obtains its configuration file from the TFTP server.

- CSCeb40099

  The Cisco ATA plays an incorrect tone after unconditional call forwarding is enabled or disabled.

- CSCeb44406

  Change the behavior of the Cisco ATA to not remove all registrations.

Release 2.16.2

- CSCec04457

  The *nonce* value of the SIP *Auth* header in a REGISTER/INVITE message can now support a maximum of 128 characters (previous maximum was 64 characters).

Resolved H.323 Issues

This section lists the issues in previous releases of the Cisco ATA that are resolved in Cisco ATA Release 2.16 or later for H.323 only:

- Release 2.16, page 18
- Release 2.16 Build 030509a, page 18
- Release 2.16.1, page 19

Release 2.16

- CSCdz28921

  The Cisco ATA 188 (version 2.15) does not mark H.323 signaling packets that are being sent to the Cisco Call Manager.

- CSCdz36431

  Cisco ATA-to-Cisco ATA calls destined for the value of the UID1 parameter instead go to the UID0-configured value.

- CSCea12163

  Direct IP calling fails from the Cisco ATA **Phone 1** port to the Cisco ATA **Phone 2** port.

- CSCea33939

  One-way audio exists on calls made between a Cisco ATA running H.323 version 2.14 and a Cisco ATA running SCCP 2.15.ms or greater.

Release 2.16 Build 030509a

- CSCea46231

  The Cisco ATA188 stops answering VoIP calls after receiving invalid packets.

- CSCea48726

  The Cisco ATA188 resets after receiving invalid packets.

- CSCea62130

  The Q931 and H323 setup fields are not correctly modified in some instances.

- CSCea86925

  When the Cisco ATA receives a Setup message with the bearer cap set as “Unrestricted Digital Information,” the Cisco ATA responds with a release-complete message that contains an incorrect cause information element.

  In this build, Bit 16 of the ConnectMode parameter has been added to resolve this issue. If this bit is set to 1, the Cisco ATA respond with a release-complete message that contains *65* as the cause information element for a setup message that has *unrestricted digital information* bearer capability.

Release 2.16.1

- CSCea48726

  The Cisco ATA resets after receiving an invalid packet.

Resolved SIP and H.323 Issues

This section lists the protocol-generic issues in previous releases of the Cisco ATA that are resolved in Release 2.16 or later for both SIP and H.323:

- Release 2.16, page 19
- Release 2.16.1, page 20

Release 2.16

- CSCdz02790

  Duplexity mismatch occurs in Cisco Discovery Protocol (CDP) information.

- CSCdz09747

  Standard G3 fax transmissions are failing because the echo canceller is disabled when it should remain enabled.

- CSCdz43469

  G.711 frame size is fixed at 20 ms and cannot be reconfigured.

- CSCdz46738

  The Reset and Refresh commands cannot be individually executed if web access is disabled.

- CSCdz47475

  The Cisco ATA plays a garbled voice configuration menu prompt.

- CSCdz54919

  The Cisco ATA does not allow caller ID to display on a phone that has two lines.

- CSCdz88561

  The Cisco ATA 186, when running v2.15 ata186 (Build 020911b), permits the **http://<*ATA IPaddress*>/reset** command to take effect without requiring a username or password.

- CSCea55168

  Out-of-band DTMF RTP packets are not sent repeatedly for redundancy purposes, as with the Cisco AS5350.

- CSCea55279

  Special digits for restricted and unknown calls are not sent to a caller ID display device that supports DTMF signaling.

Release 2.16.1

- CSCeb15288

  The Cisco ATA does not recognize DTMF digits sent from KROWN 2000DX TTY.

- CSCeb43977

  OpFlags bit 14 for controlling DNS name resolution is wrong. The correct bit number is 13.

Release 2.16.2

- CSCec04279

  Bell core GR30-core requires FSK amplitude to be between -12 and -15 dBm. The caller ID FSK level has been adjusted to -13 dBm.

- CSCec34508

  The stuttering dial tone on the Cisco ATA is used to indicate both message waiting and unconditional call forwarding. In releases prior to 2.16.2, the Cisco ATA could indicate an incorrect status by turning off the stuttering dial tone if either unconditional call forwarding was disabled or if no messages existed.

  In release 2.16.2, the stuttering dial tone will remain on if either unconditional call forwarding is enabled or if messages exist.

Open Issues in Cisco ATA Release 2.16.2

This section contains the following topics:

Open Issues for SIP

There are no SIP-specific open issues in Cisco ATA Release 2.16.2.

Open Issues for H.323

There are no H.323-specific open issues in Cisco ATA Release 2.16.2.

Open Issues for SIP and H.323

There are no open issues for SIP and H.323 in Cisco ATA Release 2.16.2.

Related Documentation

Use these release notes in conjunction with the documents located at this index:

- *ATA 186 and ATA 188 Analog Telephone Adaptor*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/ata/index.htm

Obtaining Documentation

The following 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 the following URL:

http://www.cisco.com

Translated documentation is available at the following 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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 21.