SIP Protocol Subscriber Features

Revised: May 3, 2007, OL-5352-12

Cisco BTS 10200 supports SIP subscribers such as SIP phones compliant with RFC 3261 or RFC 2543. The SIP protocol support in Cisco BTS 10200 provides the capability to provision subscriber features, and to allow SIP devices to work with the Cisco BTS 10200 Softswitch. This chapter describes the subscriber features.

Note For quick-reference tables listing the Subscriber features, see Chapter 1.

This section covers the following topics:

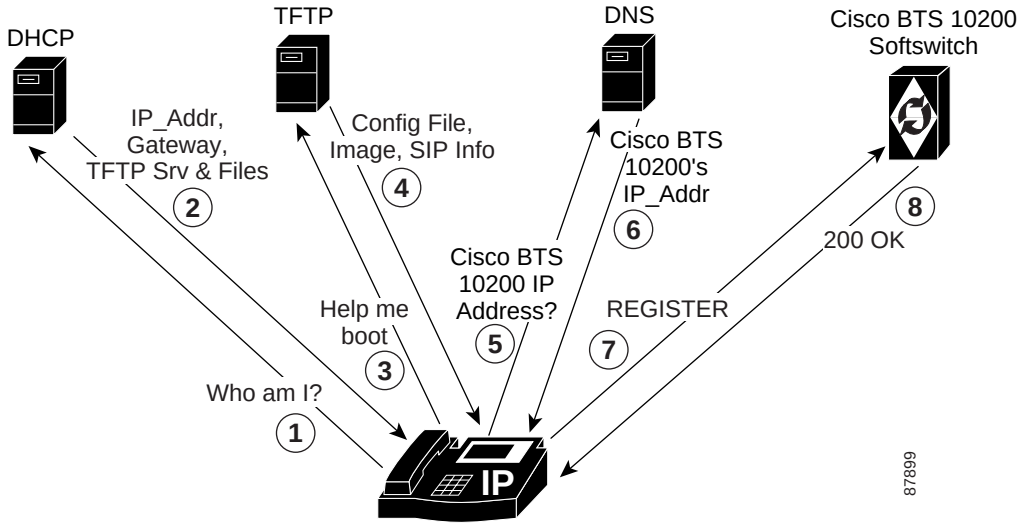
SIP Phone Initialization

Figure 2-1 shows SIP phone initialization on bootup.

The image shows actions that occur external to Cisco BTS 10200—it does not show how Cisco BTS 10200 controls SIP initialization, but rather is representative of how a client may establish its identity with Cisco BTS 10200.

The numbers in the image reference the numerical order in which the sequence would occur.

Figure 2-1 SIP Phone Initialization



SIP Devices

The following Cisco SIP devices, when running a SIP application image, are supported on Cisco BTS 10200:

- Cisco ATA 186/188
- Cisco IP Phone 7905
- Cisco IP Phone 7912
- Cisco IP Phone 7940
- Cisco IP Phone 7960
- Cisco LINKSYS Phone Adapter PAP2

For more information on provisioning devices, see the Provisioning SIP Devices section in the *Cisco BTS 10200 SIP Protocol Provisioning Guide*.

You can find the detailed step-by-step administration guide for the Cisco ATA 186/188 adaptors at:

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

You can find the detailed step-by-step administration guide for the Cisco 7905/7912 phones at:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7905g/addprot/index.htm

You can find the detailed step-by-step administration guide for the Cisco 7940/7960 phones at:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/sip7960/sadmin31/index.htm

For multiple line SIP phones, each line must be provisioned with a DN/Subscriber entry in the Cisco BTS 10200 Softswitch.

SIP Registration and Security

SIP subscribers use the SIP REGISTER method to record their current locations with Cisco BTS 10200. Registering clients may specify an expiry time for the contacts being registered. However, Cisco BTS 10200 has a minimum and maximum acceptable duration which are configurable.

Note Third-party registration is not supported.

It is possible to register multiple contacts for a single Address of Record (AOR); however, if multiple contacts are registered for a single subscriber, Cisco BTS 10200 uses only the most recently registered contact to deliver the call to that subscriber. For this reason, multiple contacts are not supported.

Note Only one contact should be registered for an AOR.

When a SIP user attempts to register or set up a call, the Cisco BTS 10200 challenges the SIP subscriber based on the Serving Domain Name table. If the Serving Domain Name Table indicates that authentication is required, the Cisco BTS 10200 challenges the SIP request (Register/INVITE) according to the authentication procedures specified in the SIP Protocol RFC 3261). If the Cisco BTS 10200 receives valid credentials, then the authenticated AOR from the User Authentication table identifies the subscriber based on the Address of Record to Subscriber table.

Registration creates bindings in Cisco BTS 10200 that associate an AOR with one or more contact addresses.

The registration data is replicated on the standby Cisco BTS 10200 Softswitch. The Cisco BTS 10200 imposes a minimum registration interval as a provisionable value. If the expiration duration of the incoming registration request is lower than the provisioned minimum, a 423 (Interval Too Brief) response is sent to the registering SIP endpoint.

The Cisco BTS 10200 generates a warning event when a request from a client fails authentication. This can be indicative of a provisioning error, or of an attempt by an unauthorized client to communicate with the Cisco BTS 10200.

The contacts registered for an AOR may be looked up using the status command, as demonstrated by the following example.

```
CLI>status sip-reg-contact AOR_ID=4695551884@sia-SYS44CA146.ipclab.cisco.com

AOR ID -> 4695551884@sia-SYS44CA146.ipclab.cisco.com
USER -> 4695551884
HOST -> 10.88.11.237
PORT -> 5060
USER TYPE ->  USER_PHONE_TYPE
EXPIRES -> 3600
EXPIRETIME -> Thu Jan 22 14:33:36 2004

STATUS -> REGISTERED CONTACT

Reply :Success:
```

Enhanced SIP Registration

Enhanced SIP Registration was added to Release 4.5.x to ensure that a SIP REGISTER message to the Cisco BTS 10200 is from a provisioned endpoint, that is, an endpoint with a provisioned secure Fully-Qualified Domain Name (FQDN) or IP address. The feature also ensures that the source IP address and contact parameter for all originating calls are from the provisioned SIP endpoint, and that no calls can originate from an unregistered endpoint.

In previous releases, SIP endpoint registration was based on Address of Record (AOR), UserID and Password; there was no verification of the origination of the REGISTER message. Certain service providers may prefer that the source IP address of SIP requests be verified against a provisioned FQDN of the endpoint to address the possibility of theft of VoIP service.

The Cisco BTS 10200 can indicate SECURE_FQDN provisioning for specified SIP term-type subscribers. This indication consists of specifying a Fully Qualified Domain Name (FQDN) with the Subscriber Address of Record (AOR). The FQDN is the address/location of the SIP endpoint and is added to the AOR table. The FQDN will not have a service port.

To enable or disable SECURE_FQDN on a successful registered subscriber:

1. Take AOR Out-Of-Service to remove all registered contact.
2. Enable or disable SECURE_FQDN for the subscriber.
3. Bring AOR back In-Service.
4. Reboot the ATA.

Note For the SECURE_FQDN provisioning commands, see the "Provisioning Secure FQDN of a SIP Endpoint" section in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide.*

A subscriber with the secure FQDN feature enabled has the following characteristics:

- One and only one AOR is associated to the endpoint.
- Does not have any static-contact associated with it.
- UserId and Password Authentication are supported.
- One FQDN (specified without service port).
- The DNS lookup of the FQDN should result in one and only one IP address.
- Cannot place or receive a call unless successfully registered.

Example:

This example considers a case in which a VoIP subscriber (Subscriber 1) uses following options for the User ID, password and phone number:

- user-id-1
- password-1
- phone-no-1

Without security, another VoIP subscriber, Subscriber 2, could access Subscriber 1's information (perhaps by getting a Cisco ATA configuration file with the encryption key in clear text, and then getting the full configuration file with all the data). Subscriber 2 could then register to the Cisco BTS 10200 with Subscriber 1's combination of user-id-1, password-1 and phone-no-1, as well as Subscriber 2's own

IP address. Without the secure FQDN feature, the Cisco BTS 10200 would accept this information unless specific measures were taken, and Subscriber 2 could steal service and make calls on behalf of Subscriber 1.

Provisioning Commands

In Release 4.5.x, a new field, SECURE_FQDN, was added to the SUBSCRIBER and AOR2SUB tables. A non-null value in the field indicates that the SECURE_FQDN validations apply to all SIP messages received from the endpoint associated with that AOR.

- The SECURE_FQDN value can be specified on a subscriber only if the AOR for the subscriber is OOS. When an AOR is taken Administratively Out of Service (OOS), its registered contacts are deleted.
- A static contact cannot be specified for a SECURE_FQDN subscriber. Any existing static contact record for an AOR must be deleted before the subscriber can be made a SECURE_FQDN SIP endpoint.
- The SECURE_FQDN in the AOR2SUB table is stored both in the ORACLE database and the shared memory.

AOR2SUB records cannot be added or deleted directly. AOR2SUB records are added by specifying the AOR ID on a subscriber record.

Operations

The following checks were added to Release 4.5.x. If any of the following conditions are not met, the request is rejected, and an alarm is generated.

No Calls To or From an Unregistered Secure-Provision SIP Endpoint

An Unregistered secure-provision SIP endpoint cannot originate or receive calls.

Third Party Registrations for Secure FQDN Endpoint Not Allowed

Third party registrations for secure FQDN endpoint are not allowed.

Cisco BTS 10200 Challenges Registration

On receiving a REGISTER message from a secure-provision SIP endpoint, the Cisco BTS 10200 challenges the registration asking for authentication. Verification of the resend REGISTER message with UserId and Password is as follows, after the UserId and Password is authenticated:

- Ensure that there is only one contact in the contact header.
- Ensure that the source IP address of the REGISTER message is the same IP address of the provisioned FQDN for that endpoint.
- Ensure that IP address or the FQDN of the contact is the same as the provisioned FQDN for that endpoint.

If any of these conditions are not met, registration is rejected and a security event and alarm is generated, indicating that the source of the registration is illegal.

The contact address can verify all subsequent SIP request source IP address of the request from the endpoint until the registration expired or is deregistered.

Registration Expires

If the registration expires or the end point de-registers, the registration process in the "Cisco BTS 10200 Challenges Registration" section on page 2-5 occurs before any new calls are accepted.

Call Originates From or Terminate to a Secure-Provision SIP Endpoint

When a call originates from or terminates to a secure-provision SIP endpoint, the system:

1. Authenticates the user ID and password on all messages requiring authentication.
2. If the Contact header is available, the system ensures that only one contact is present, and that it has the same IP address or FDQN of the provisioned endpoint.
3. All messages sent by the endpoint and the Source IP address of the message are the same as the internal cache contact address (for example, the cache contact address is the contact obtained during registration).
4. Response from an endpoint that has a contact header must conform to the bullet 2, above.

Call Processing

The SIP Application in Cisco BTS 10200 implements the secure provisioning feature for all incoming SIP messages (requests and responses) from SIP endpoints.

When a SIP request message is received from a SIP endpoint, and Auth_Rqed=Y for the serving domain, the request is challenged. When the request is resubmitted with credentials, the AOR of the authenticated SIP endpoint is used to perform the SECURE_FQDN validation, provided a SECURE_FQDN value is provisioned in the AOR2SUB record. If Auth_Reqd=N, the SECURE_FQDN validation is performed without the request being challenged.

Validation

The validation processing for a SIP request, from a SIP endpoint provisioned with this feature, is as follows:

1. The SECURE_FQDN validation occurs on every request (including CANCEL/ACK).
2. The SECURE_FQDN is verified to have a DNS resolution, if it is a domain name.

   If not, a 500 Internal Server Error response is returned.
3. The DNS resolution for the SECURE_FQDN is verified to yield a single IP address Secure-IP1.

   If not, a 500 Internal Server Error response is returned.
4. The Source IP address of the packet is verified as identical to Secure-IP1.

   If not, a 403 Forbidden response is returned.
5. If the Request is a Register, it is verified to have a single Contact header.

   If not, a 403 Forbidden response is returned.
6. If the SIP request is an initial INVITE (including INVITE resubmitted with credentials), it is verified that there is an unexpired registered contact for the AOR.

   If not, a 403 Forbidden response is returned.
7. When a Contact header is present, the Contact FQDN/IP address of the request is verified to yield a single IP address Secure-IP1.

   If not, a 500 Internal Server Error response is returned.

8. The IP address of the Contact host is verified as identical to the IP address Secure-IP1 of the SECURE_FQDN.

   If not, a 403 Forbidden response is returned.

9. The provisioning of a static contact on a AOR is not disabled, but any provisioned value is ignored because of the SECURE_FQDN validation rules. A static contact is irrelevant for SECURE_FQDN AORs, since the SIP request is denied if no registered contact exists.

10. The To and From header URLs in a REGISTER are verified as identical, for SECURE_FQDN subscribers. This is to block third party registration.

Received SIP Response Message

When a SIP response message is received from a SIP endpoint, the following occurs:

1. The Source IP address of the packet is verified as identical to Secure-IP1.

   If not, the response is dropped. This has the same result as the non-receipt of that response, such as a call failure.

2. When a Contact header is present on a reliable 1xx or 2xx response, the Contact FQDN/IP address of the response is verified to resolve to the Secure-IP1.

   If not, the response is dropped. This has the same result as the non-receipt of that response, such as a call failure.

3. The response for a BYE sent by Cisco BTS 10200 is not validated. This is the least interesting point in a call for theft.

Rules for Sending a SIP INVITE Message from Cisco BTS 10200

When a SIP INVITE message is sent to a SIP endpoint, the following occurs:

1. The INVITE is sent to the registered contact of the endpoint. If there is no registered contact or if the registered contact has expired, the INVITE is not sent and the call is declined.

2. Any static contact provisioned for the subscriber is ignored.

Note Provisioning of static contact is not allowed for secure SIP endpoints; therefore, this is merely due diligence.

Validation of ACK Request

When a SIP ACK message is received from a SIP endpoint, the following occurs:

1. The ACK for a 200-class response is validated like any other SIP request.

2. The ACK for a failure response (3xx or higher) is not validated.

Measurements

This section lists the measurements that are new, modified, or deleted as a result of the features covered by this document. The measurements are grouped into logical categories for easy identification.

Note See the Measurements section for a complete list of all traffic measurements.

The following TMM counters were added to Release 4.5.x:

- A SIA-SECURE_FQDN-VIOLATION-REQ counter will be incremented when a SIP request fails the validation for secure SIP endpoints.
- A SIA-SECURE_FQDN-VIOLATION-RESP counter will be incremented when a SIP response fails the validation for secure SIP endpoints.

Events and Alarms

A Warning event is raised when a SIP a request or response fails the validation for secure SIP endpoints. The alarm has the following attributes:

Component Id: Security

Type: SECURITY(6)

DESCRIPTION: Secure SIP Endpoint Validation Failure

SEVERITY: WARNING

INITIAL RELEASE: 4.5

THRESHOLD: 100

THROTTLE: 0

END-CUSTOMER PERCEPTION: No impact

DATAWORDS:

string: AOR

string: Secure Fqdn

string: Source IP Address

string: Violation Description

SIP User Authentication

The Cisco BTS 10200 Softswitch can act as an authentication server. Authentication is enabled on the serving domain through provisioning.

Whenever a SIP request is received from a SIP subscriber, the request is authenticated to ensure it is indeed from an identified user. Authentication also enables request authorization, since users may be authorized to perform only specific requests.

The following examples are the functional scenarios in which authentication is required:

1. When a SIP user registers a contact with the Cisco BTS 10200 Registrar using a REGISTER request.
2. When a SIP user initiates a call using an INVITE request.
3. When a SIP user sends any request in an ongoing call. Examples might include:
   - Re-negotiation of the call parameters using a re-INVITE
   - Terminating the call using a BYE
   - Initiating a call transfer using a REFER
4. When a SIP user sends a request outside a dialog. Example: OPTIONS.

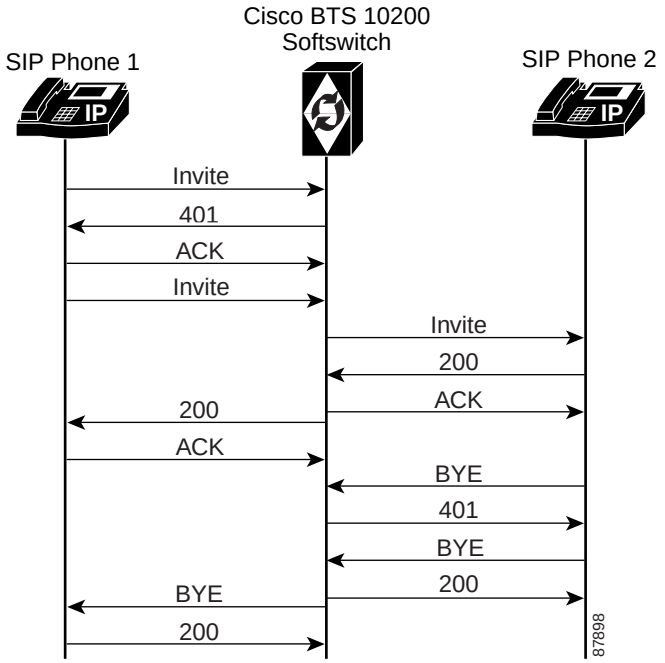
The following new tables have been defined for SIP subscribers, which are pertinent to Authentication:

- AOR
- Serving Domain
- Auth-Realm
- User-Auth

See Chapter 5, "Database Tables" for more information about the tables.

Figure 2-2 shows how an incoming request is processed, and the role of the Authentication Service in the Cisco BTS 10200.

Figure 2-2 Authentication and Processing of an Incoming Request (e.g. INVITE)



The BTS 10200 validates the hostname of the ReqUri of every incoming SIP request against the list of names provisioned in the Serving-Domain-Name table. The BTS 10200 hostname used by devices (in the ReqUri), when sending requests to the BTS 10200, should be provisioned in the Serving-Domain-Name table of that BTS 10200. If a name is not provisioned (and therefore not found) in the Serving-Domain-Name table, the BTS 10200 rejects the SIP request with a "404 Not Found ReqUri Serving Domain" response.

The BTS 10200 authenticates IP phones by using the MD5 digest defined in RFCs 3261 and 2617. The BTS 10200 verifies a user's credentials on each SIP Request from the user. For more information, see the "User Authentication" section on page 5-35.

Cisco BTS 10200 Softswitch-Based Features

Softswitch-based features are directly provided by the Cisco BTS 10200 Softswitch. SIP phones may provide some features on their own; for information on the features provided by the different SIP phones, see the SIP phone administration guides.

This section describes Softswitch-based features entirely provided by the Cisco BTS 10200 Softswitch.

For information on MGCP features in previous Cisco BTS 10200 releases, and how they compare with SIP features in Release 4.5.x, see Appendix A, "MGCP Features vs. SIP Features."

Note Cisco BTS 10200 Softswitch Announcements are customizable on a business group basis. If an announcement is not provisioned or cannot be played, a reorder tone is played.

Activation and Deactivation of Anonymous Call Rejection

Anonymous Call Rejection (ACR) activation and deactivation is supported through a feature (*) code. It is supported on a SIP endpoint, and supports single-stage dialing.

ACR has multiple activation options as follows:

- Activated permanently at subscription time by service provider—When ACR is first provisioned by the service provider, it is active immediately by default. To assign this feature in the deactivated state, configure the subscriber-feature-data table for that subscriber to make ACR deactivated.
- Activated by user:
  - The user lifts the handset, and listens for a dial tone.
  - The user presses the activation Vertical Service Code (VSC); for example, typically *77 in North America. If ACR can be activated, the system returns a success announcement.
  - ACR is now activated, and will stay active until it is deactivated.

Note If the user tries to activate ACR when it is already active, the system treats the new activation attempt as a new attempt.

ACR deactivation options are as follows:

- Service provider deactivation at user request.
- Deactivated by user:
  - The user lifts the handset and listens for a dial tone.
  - The user presses the deactivation VSC; for example, typically *87 in North America. The system responds with a success announcement.
  - ACR is now deactivated, and will stay inactive until it is activated.

Note If the user tries to deactivate ACR when it is already deactivated, the system accepts and processes the new deactivation attempt as a new attempt.

For more information, see the Anonymous Call Rejection section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Billing

The Cisco BTS 10200 Softswitch provides call data for billing on SIP calls. Specific fields are supported in the call detail data records for calls that originate or terminate on a SIP trunk or subscriber. For detailed information on billing management and data, see the *Cisco BTS 10200 Softswitch Billing Interface Guide*.

CALEA Call Content

CALEA is not available for SIP subscribers.

Call Forwarding

For more information, see the Call Forwarding Features section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Call Forwarding Activation and Deactivation

Activation and deactivation of call forwarding features uses the star code. Alternately, the feature may be activated or deactivated by using the Services key on certain phones.

With SIP support, the call forwarded to number can be a Centrex extension number (only applicable for business users) or an E.164 number.

Note Forwarding to a URL (AOR) is not supported.

SIP subscribers do not hear a final dial tone upon completing activation or deactivation. Instead, an announcement plays for the subscriber, indicating that the status of the forwarding feature is being activated or deactivated. This is irrespective of the Final Stage Dial Tone (FDT) flag (Y/N) provisioned for these features.

Call Forwarding to an E.164 Number or an Extension Number

In Release 4.5.x, activation is accomplished using single-stage dialing. This applies to all activation and deactivation.

Calling Name and Number Delivery

Calling number delivery (CND) provides the SIP subscriber endpoint with the calling number of an incoming call. Calling name delivery (CNAM) provides the endpoint with the name of the calling party.

CND

The calling party number, if available, is delivered in the From: header of the outgoing INVITE from the BTS 10200 to the terminating SIP phone. The number is delivered to the SIP phone even if the CND feature is not provisioned for the subscriber. The delivered information is as follows:

- If the calling number is available, and the presentation indication is *not restricted*, the number is populated into the user information portion of the From: header.
- If the calling number is available, and the presentation indication is *restricted*, the user information portion of the From:header is set as “Anonymous.”
- If the calling number is not available, the user information portion of the From:header is left empty.

CNAM

The calling party name is delivered in the outgoing INVITE from the BTS 10200 to the terminating SIP phone only if the CNAM feature is provisioned for the SIP subscriber. The delivered information is as follows:

- If the calling number and name are available, and the presentation indication of both the calling number and calling name are *not restricted*, the calling name is populated into the display name field of the From: header.
- If the calling number and name are available, and the presentation indication of either calling number or calling name is *restricted*, the display name field of the From:header is set as “Anonymous.”
- If the calling name is not available, the display name field of the From:header is left empty.

For more information, see the Calling Number Delivery section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide, and the CND and CNAM sections in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Caller ID Delivery Suppression

The treatment for caller’s identity is based on presence of “anonymous” in the Display-Name field of From header in the INVITE. Caller Identity presentation (allowed/restricted) information for SIP subscribers is not maintained in the Cisco BTS 10200 Softswitch database.

This information is maintained on the individual phones, and can be provisioned through the phones’ softkeys. If the caller’s identity is restricted in the incoming SIP INVITE message, the presentation is suppressed. You can override permanent restriction on the phone by the caller dialing a feature (*) code on a per-call basis. This is a single-stage dialing for SIP subscribers.

Called Party Termination

Called Party Termination is Not Available/Not Reachable

This feature was introduced in a previous Cisco BTS 10200 Softswitch release. There are no differences when provisioning the feature for SIP.

Called Party Termination is Not Registered

This feature was introduced in a previous Cisco BTS 10200 Softswitch release. There are no differences when provisioning the feature for SIP.

Cisco BTS 10200 Supplementary Vertical Service Code Features

The following Cisco BTS 10200 Vertical Service Code (VSC) features are supported on SIP endpoints:

- Calling identity delivery and suppression (per call)—suppression part (CIDSS), calling identity delivery and suppression (per call)—delivery part (CIDSD)
- Calling name delivery blocking (CNAB)
- Outgoing call bearing activation (OCBA), outgoing call bearing deactivation (OCBD), outgoing call bearing interrogation (OCBI)
- Call forwarding unconditional activation (CFUA), call forwarding unconditional deactivation (CFUD), call forwarding unconditional interrogation (CFUI)

Note Reminder ringback cannot be enabled for SIP subscribers. If turning on the Call Forward Unconditional (CFU) feature for a SIP subscriber, make sure that reminder ring capability is turned off. This should be done at a subscriber level.
The command format would be as follows at the feature level:
add feature fname=CFU; tdp1=TERMINATION_ATTEMPT_AUTHORIZED; tid1=TERMINATION_ATTEMPT_AUTHORIZED; ttype1=R; fname1=CFUA; fname2=CFUD; type1=MCF; value1=Y; type2=RR; value2=N; description=CFU MCF=multiple call forwarding allowed, RR=ring reminder;

feature_server_id=FSPTC235;

And at the Subscriber feature level:
add subscriber-feature-data sub_id=sip_sub2;FNAME=CFU;type2=RR;VALUE2=N

- Call forwarding on no answer variable activation (CFNAVA), call forwarding on no answer variable deactivation (CFNAVD), call forwarding on no answer interrogation (CFNAI)
- Call forwarding on busy variable activation (CFBVA), call forwarding on busy variable deactivation (CFBVD), call forwarding on busy variable interrogation (CFBI)
- RACF Pin Change

Note SIP client/handset dialing sequence: Using this feature involves dialing the VSC digits, followed by additional dialing-keys representing the parameters for the feature call. For SIP endpoints, all the digits are dialed at a stretch without waiting for an intervening response tone from the Softswitch (i.e., in between the VSC code and additional dialing-keys).

Customer Access Treatment

This feature was introduced in a previous Cisco BTS 10200 Softswitch release. There are no differences when provisioning the feature for SIP.

Customer-Originated Trace

This feature was introduced in a previous Cisco BTS 10200 Softswitch release. There are no differences when provisioning the feature for SIP.

For more information, see the Customer Originated Trace section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Direct Inward Dialing

This feature was introduced in a previous Cisco BTS 10200 Softswitch release. There are no differences when provisioning the feature for SIP.

For more information, see the Direct Inward Dialing section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Direct Outward Dialing

With the Direct Outward Dialing (DOD) service, a station user can place external calls to the exchange network without attendant assistance by:

1. Dialing the DOD (Public) access code (usually the digit 9)
2. Receiving a second dial tone
3. Dialing the external number (i.e., outside the customer group)

Access to the DOD feature is subject to station restrictions.

Note For IP phones, the second dial tone is provided by the phone itself. However, the prefix code is presented to the Cisco BTS 10200 along with the DDD number in the INVITE message. Secondary dial-tone capability is dependent on the SIP device used. This is achieved by provisioning a suitable dial plan configuration on the phone.

For more information, see the DOD for PBX section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Do Not Disturb

Do Not Disturb (DND) enables a user to temporarily busy out a station when the feature is activated.

If no call forwarding features are activated, calls to the station are routed to busy treatment. Preferably, this feature should be provided on the Cisco BTS 10200 Softswitch because of feature interaction with advanced features like executive override.

This is a single stage dialing activation feature. The Alert-Info header plays the result of activation/deactivation, Success: confirmation tone and Failure: messages.

For features (such as DND) that can be fully provisioned on the Cisco BTS 10200 Softswitch or on the phone, provision either one of the devices to enable the feature.

Caution Do not attempt to provision the feature on both the switch and the phone, because this can cause conflicts.

For more information, see the Do Not Disturb section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Emergency Call

Emergency Call (911) is supported for SIP endpoints with one caveat: If the calling party (SIP subscriber) disconnects the call, the called party control is not available. Otherwise, the call will be released. Expanded emergency service (E911) does not require this, but basic emergency service (911) does. Both 911 and E911 are supported for MGCP endpoints.

Note PSAP is selected based on default user location. No mobility is supported.

For more information, see the Emergency Services (911) section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

E.164 and Centrex Dialing Plan (Extension Dialing)

Cisco BTS 10200 supports E.164 and Centrex Dialing Plan (Extension dialing) addressing from SIP User Agents. AOR addressing is not supported in Release 4.2.

The SIP phone's dial plan must be configured so that it considers the number of digits in the Centrex group. Each Centrex group should have its own separate dial plan.

Example 2-1 A SIP URL with E.164 addressing

```
sip:4695551234@rcdn.cisco.com;user=phoneA sip:50603@rcdn.cisco.com;user=phone
```

The number of digits used for Centrex dialing can be provisioned within a range of 1 through 7 digits.

Incoming and Outgoing Simulated Facility Group

This feature was introduced in a previous Cisco BTS 10200 Softswitch release. There are no differences when provisioning the feature for SIP.

For more information, see the Features for Centrex Subscribers Only section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Interworking

Release 4.5.x supports the following interworking combinations between SIP subscribers and:

- H.323 trunks
- SIP trunks
- PSTN (SS7, ISUP)
- ISDN
- MGCP subscribers

Multiple Directory Numbers

This feature was introduced in a previous Cisco BTS 10200 Softswitch release. For information about how MDN works with SIP, see the SIP Endpoint Caveats section.

For more information, see the Multiple Directory Numbers section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Operator Services (0-, 0+, 01+, 00 Calls)

This feature was introduced in a previous Cisco BTS 10200 Softswitch release. There are no differences when provisioning the feature for SIP.

For more information, see the Operator Services section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Outgoing Call Barring

This feature was introduced in a previous Cisco BTS 10200 Softswitch release. There are no differences when provisioning the feature for SIP.

For more information, see the Outgoing Call Barring (OCB) section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Remote Activation of Call Forwarding

This feature was introduced in a previous Cisco BTS 10200 Softswitch release. There are no differences when provisioning the feature for SIP.

For more information, see the Remote Activation of Call Forwarding section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

SIP Endpoint Caveats

The following Cisco BTS 10200 supported supplementary features have caveats when compared with an MGCP endpoint behavior for the same feature:

- 911—Only E911 (without the suspend procedure for 45 minutes) support. Basic 911 with suspend procedure is not supported.
- Call transfer (CT)—For SIP phones, this feature is provided as part of REFER support on Cisco BTS 10200. See REFER feature below for more details.

- Distinctive alerting call waiting indication (DACWI)—Ringing part supported by Cisco BTS 10200. Cisco BTS 10200 sends distinctive alerting request for Call Waiting scenario. Some SIP phones interpret it, and play distinctive call-waiting tone; other phones do not.
- Distinctive ringing/call waiting (DRCW)—Ringing part supported by Cisco BTS 10200. Cisco BTS 10200 sends distinctive alerting request for Call Waiting scenario. Some SIP phones interpret it, and play distinctive call waiting tone; other phones do not.
- Multiple directory numbers (MDN)—Ringing part supported by Cisco BTS 10200. Cisco BTS 10200 sends distinctive alerting request for Call Waiting scenario. Some SIP phones interpret it, and play distinctive call waiting tone; other phones do not.
- Call waiting deluxe activation (CWDA), call waiting deluxe activation (CWDD), and call waiting deluxe interrogation (CWDI)—Depends on whether functionality is supported by the phone.
- Account-code/Auth-code capability is not supported for the Class of service feature offered to SIP subscribers. However, this capability is available to MGCP subscribers.

SIP Subscriber to SIP Calls

SIP subscribers must present valid credentials on a SIP INVITE message in order to place calls.

In Release 4.5.x, Cisco BTS 10200 allows SIP subscribers to call other SIP subscribers or SIP trunks connected to Cisco BTS 10200. The provisioned dial plan determines whom a subscriber may call. A SIP subscriber may receive a call as long as the subscription's registration is current, or a static registration has been provisioned. A SIP subscriber may call any SIP endpoint hosted by a trunk that was provisioned on Cisco BTS 10200.

Type of Service

The SIP Type of Service (ToS) feature provides the ability to configure the Cisco BTS 10200 such that SIP signaling traffic is sent at a desired priority over IP. This is important because SIP messages travel over the same network as the voice traffic. If this network is congested, the voice data may delay the SIP signaling packets, causing unnatural delay when calls are set up. Raising the SIP packets priority in relation to other traffic reduces the delay.

The ToS value for messages sent to SIP subscribers can be set on a system-wide basis—this applies to all subscribers. The policy is selected in the CA-CONFIG table. If the ToS entries are not provisioned in CA-CONFIG table, the following defaults apply:

- Precedence - FLASH (3)
- Delay = low (Y)
- Throughput = normal (N)
- Reliability = normal (N)

Note These are the recommended values; these values should be changed only after careful consideration, or if there is a specific need.

Caution If you change any parameters in the ca-config table, these changes do not take effect until the CA platform switches over or restarts.

User-Level Privacy

User-level privacy is provisioned in the Subscriber table. Setting the privacy parameter to “user” directs the system to apply the user-provided privacy information. This setting (privacy=user) applies only to SIP endpoints that are capable of including privacy information.

Voice-Mail Support

Cisco BTS 10200 supports the following voicemail features:

- Voice-mail deposit
- Notification
- Retrieval
- Callback

Voice-mail systems are configured as SIP trunks in Cisco BTS 10200. For voice-mail operation, see Chapter 4, “Voice-Mail Support.”

SIM Memory Audit

The SIM memory audit is done periodically for the active feature relationships to clear any stale relationships. Audits on the entire feature relationship table are also performed at a configurable fixed time every day to clean up the orphaned table elements.

SIP Dynamic Memory Audit

Note The SIP dynamic memory audit is a new feature for Release 4.5.x. It is automatically enabled on a new install of Release 4.5.x, but not in previous releases upgrading to Release 4.5.x. If upgrading to Release 4.5.x from a previous release, you must enable the feature.

The SIP dynamic memory audit checks the resources for call processing and call registration, and maintains those resources through both periodic and scheduled checks.

For example, if a call is connected to a remote endpoint (such as a trunk) and terminates abnormally, or if call connectivity is lost, the Cisco BTS 10200 recovers the resources on a periodic basis (approximately every one to two hours) by running an audit. During the audit, if no signalling has occurred on a call for more than an hour, the liveness of the call is checked by sending a re-INVITE or an UPDATE message to the SIP parties in the call.

The scheduled audit runs daily, and checks any contacts registered with SIP subscribers to ensure they have been refreshed. The SIP phone subscriber registry is expected to refresh regularly; however, if it is not, the Cisco BTS 10200 runs a scheduled audit once a day to reclaim stale resources associated with those registrations.

Note The feature requires no provisioning; use the audit default values. If you do want to change the values, consult with your Cisco representative before doing so.

For provisioning options, see the Session Timers section in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

Billing

A new value was added to the Appendix B: Call Termination Cause Codes in the Cisco BTS 10200 Softswitch Billing Guide. The new call termination cause code is called “NE Cause Audit Release” and its value is 901.

Alarms and Events

The following alarms were added or modified due to the SIP audit memory:

AUDIT(10)

DESCRIPTION: Call Data Audit Complete

SEVERITY: INFO

INITIAL RELEASE: 4.5

LAST RELEASE MODIFIED IN: 4.5

THRESHOLD: 100

THROTTLE: 0

END-CUSTOMER PERCEPTION: No impact

DATAWORDS:

Audit Information - STRING [256]

PRIMARY CAUSE:

A memory audit has completed
PRIMARY ACTION:

Check if any Call Blocks freed as a result of Audit. An investigation for root cause may be useful.

AUDIT(19)

DESCRIPTION: Recovered Memory of stale call

SEVERITY: WARNING

INITIAL RELEASE: 4.5

LAST RELEASE MODIFIED IN: 4.5

THRESHOLD: 20

THROTTLE: 0

END-CUSTOMER PERCEPTION: Lost or errant billing data

DATAWORDS:

Stale Memory Release Info - STRING [128]

PRIMARY CAUSE:

Loss of communication with originating or terminating side.

PRIMARY ACTION:

Check if adjacent network element is up and having proper communication link with softswitch.
SECONDARY CAUSE:

Adjacent network device protocol error.

SECONDARY ACTION:

Check the adjacent network device protocol compatibility.

TERNARY CAUSE:

Internal Software Error.

TERNARY ACTION:

Contact Cisco Support.

AUDIT(20)

DESCRIPTION: Audit Found lost call data record

SEVERITY: MAJOR

INITIAL RELEASE: 4.5

LAST RELEASE MODIFIED IN: 4.5

THRESHOLD: 20

THROTTLE: 0

END-CUSTOMER PERCEPTION: Lost or errant billing data

DATAWORDS:

Error Text - STRING [200]

PRIMARY CAUSE:

Software error - however, the orphaned records are recovered on detection 2d.

PRIMARY ACTION:

Contact Cisco Support

Measurements

The following measurements, found in the Measurement SIA Summary (measurement-sia-summary) table, are affected by the SIP dynamic memory audits.

- SIA_AUDIT_CCB_FREED: Total CCB Cleared because of Audit – Updated when a stale CCB is freed as a result of audit.
- SIA_AUDIT_BCM_CALL_RELEASED: Total number of calls released as BCM side is inactive.
- SIA_AUDIT_REGCONTACT_FREED: Total contacts freed because of Audit.
- SIA_AUDIT_CALL_RELEASED: Total number of calls released.

An example of the Measurement SIA Summary (measurement-sia-summary):

```
report measurement-sia-summary start-time=2003-03-27 06:00:00; end-time=2003-03-27
06:30:00; call-agent-id=CA146;output-type=csv;
clear measurement-sia-summary call-agent-id=CA146;
```

Phone-Based Features

Phone-based features are provided by the SIP phone, which require provisioning on the phone.

There are some features that the phone provides standalone, without Cisco BTS 10200 support.

For features (such as DND) that are available independently on the phones and the Cisco BTS 10200 Softswitch, you can provision either device to enable the feature.

Caution When provisioning features that are available independently on the switch and the phone, use caution to avoid conflicts between the two.

The Cisco BTS 10200 Softswitch supports interface requirements (such as Re-INVITE support) that are necessary to operate features from the SIP phones, including but not limited to:

- Call Hold and Resume
- Call Waiting
- Three-Way Calling
- Cancel Call Waiting
- Call Waiting Caller ID
- CODEC Up-speeding (Depending on the SIP phone's capability to support this feature)—For feature calls between MGCP and SIP subscribers, the Cisco BTS 10200 supports CODEC up-speeding capability.

Note If CODEC re-negotiation fails (because either the SIP phone or the MGCP gateway does not support it), the call is disconnected.

- Do Not Disturb

Jointly-Provided Features

In addition to the Softswitch-based and phone-based features, Release 4.5.x also offers jointly-provided features. These are features provided jointly by the phone and by the Cisco BTS 10200. To use these features, you must provision both the phone and the Cisco BTS 10200.

These features include:

- Session Timers
- SIP Timer Values
- Reliable Provisional Responses
- Text-GUI Features
- Call Transfer (Blind and Attended)
- Distinctive Ringing
- Distinctive Ringing for Centrex DID Calls

Session Timers

Release 4.5.x enhances SIP timers and introduces the sip-timer-profile table to provision session timer values. The session timer values are provisioned in the sip-timer-profile table, then the id of the sip-timer-profile table record is specified as the Value for the ca-config record of Type=sip_timer_profile_id.

Note To configure SIP protocol and session timers in Release 4.5.x, you must use the new sip-timer-profile table. For customers upgrading to Release 4.5.x: SIP session timer values configured in the ca-config table prior to Release 4.5.x are reset to the default values after upgrading to Release 4.5.x.

This SIP extension allows for a periodic refresh of SIP sessions through a SIP re-INVITE or UPDATE request. The refresh allows the Cisco BTS 10200 SIP interface to determine if a SIP session is still active. If the session is inactive, possibly because the session did not end normally, the Cisco BTS 10200 sends a SIP BYE request and cleans up resources dedicated to the session. Stateful SIP proxies and the remote SIP endpoint handling the BYE request can clean up resources dedicated to this session as well.

Cisco BTS 10200 support for this feature follows the specifications described in the IETF draft draft-ietf-sip-session-timer-08. Session durations are configured within a range of 30 minutes to 2 hours. Cisco BTS 10200 does not allow for negotiating a session less than 15 minutes. Cisco BTS 10200 SIP interface does not impose the session timer feature be required on the remote SIP endpoint. This feature does not require the session timer capability on the remote SIP endpoint.

In the unlikely event of a call agent redundancy failover, the session timer is deactivated. This may result in eventual session expiration and call release.

This feature can be enabled or disabled for all SIP subscribers; the feature is disabled by default. Prior to Release 4.5.x, this feature was enabled by provisioning the SUB-SESSION-TIMER-ALLOWED token in the ca-config table.

In Release 4.5.x and later, the session timer values are provisioned through the MIN-SE and SESSION-EXPIRES-DELTA-SECS tokens in the sip-timer-profile table. The id of the sip-timer-profile table record is then specified as the Value for the ca-config record of Type=sip_timer_profile_id.

If the feature is enabled for a SIP subscriber, Cisco BTS 10200 (as UAC) adds, to the initial INVITE message, a supported header with a ‘timer’ value, as well as a Session-Expires header with the Refresher parameter set to ‘Uac’. Whenever the SIP call is sent from a Cisco BTS 10200 SIP subscriber, Cisco BTS 10200 specifies itself to be the refresher. If Session Timer is not supported on the remote end, the value sent in the Session-Expires header is set for the session duration. A periodic refresh request is sent at half of the negotiated Session-Expires value.

When this feature is enabled for the SIP subscriber and an initial INVITE is received by the Cisco BTS 10200 with a Supported header with ‘timer’ value and a Session-Expires header, it sends a 200 class response with a Require header specifying ‘timer,’ and a Session-Expires header and refresher parameter. The Session-Expires header contains a session duration and refresher value set to whatever was received in the initial INVITE. If refresher parameter is not received in the initial INVITE, Cisco BTS 10200 sets it to ‘Uas’ indicating Cisco BTS 10200 is the refresher. Cisco BTS 10200 sends periodic refresh request at half the negotiated session duration.

When session timer is enabled for the SIP subscriber and an initial INVITE is received by Cisco BTS 10200 without a Supported header with ‘timer’ value or a Session-Expires header, a 200 class response is sent without a Require header with ‘timer’ value, or a Session-Expires header. Cisco BTS 10200 sends periodic refresh request at half the negotiated session duration.

When session timer is disabled on the SIP subscriber and an initial INVITE is sent by Cisco BTS 10200, no Supported header with ‘timer’ value or a Session-Expires header is added, indicating to the remote SIP endpoint that the Cisco BTS 10200 does not support session timer.

When the feature is disabled on the SIP subscriber and an initial INVITE is received by Cisco BTS 10200, any session timer related headers are ignored. The 200 class response does not include a Require header with ‘timer’ value or a Session-Expires header.

Configurable parameters in the sip-timer-profile table allow the user to select the desired session duration (SESSION-EXPIRES-DELTA-SECS) and the minimum tolerable session duration (MIN-SE) if negotiated down by the remote SIP endpoint or proxy. If the parameters are not explicitly specified, the default session duration is 30 minutes and the minimum tolerable session duration allowed is 15 minutes.

A session that is not refreshed at the end of the duration interval results in a call release and session clean-up.

Note When the SESSION-EXPIRES-DELTA-SECS timer expires, the BTS 10200 might send a Re-Invite (as opposed to an Update) with the previously sent SDP. If the BTS 10200 receives a 200 OK with the SDP changed from the previously received SDP, the BTS 10200 does not send this changed SDP to the origination.

To provision these timers, see the Session Timers section in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

SIP Timer Values

Release 4.5.x enhances SIP timers and introduces the sip-timer-profile table to provision SIP timer values. The SIP timer values are provisioned in the sip-timer-profile table, then the id of the sip-timer-profile table record is specified as the Value for the ca-config record of Type=sip_timer_profile_id. If you provision the timer values for a specific trunk (by pointing to a sip-timer-profile in the softsw-tg-profile), that overrides the ca-config default.

Note To configure SIP protocol and session timers in Release 4.5.x, you must use the new sip-timer-profile table. For customers upgrading to Release 4.5.x: SIP session timer values configured in the ca-config table prior to Release 4.5.x are reset to the default values after upgrading to Release 4.5.x.

To provision these timers, see the SIP Timer Values section in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

For more information about these timers, or for common SIP term definitions from this section, see RFC3261.

The following SIP timers are available in Release 4.5.x.

- TIMER-T1-MILLI—The timer used for calculating the default values of the timers described in the SIP Session Timers section (Autocomputation) of the *Cisco BTS 10200 SIP Protocol Provisioning Guide*. T1 is an estimate of the round-trip time (RTT), defaulted at 500 ms. Nearly all of the transaction timers described in this section scale with T1, and changing the T1 adjusts the values, unless a specific value was not specified, overriding the default values calculated from timer T1 and T4.
- TIMER-T2-SECS—The timer used to cap the interval for non-INVITE requests. It is also used as the maximum retransmit interval for SIP INVITE responses.

- TIMER-T4-SECS—The timer represents the amount of time the network takes to clear messages between client and server transactions.
- TIMER-A-MILLI—The UAC timer for INVITE request retransmit interval. For example, if the value is 500 ms, the INVITE request retransmissions occur at the interval of 500 ms, 1s, 2s, 4s, 8s, 16s, 32s (assuming TIMER-B-SECS defined below is 32 seconds).
- TIMER-B-SECS—The UAC INVITE transaction timer limits the number of retransmissions for an INVITE request. For SIP TCP trunk connections, there are certain scenarios in which the Cisco BTS 10200 does not immediately detect a loss of connection to an IP address endpoint after transmitting an INVITE request. As a result, Cisco recommends provisioning the SOFTSW-TG-PROFILE Timer-B-Secs to six seconds when configuring TCP trunks, so that advancing to the FQDN's next IP address occurs in a timely manner.
- TIMER-D-SECS—The UAC timer used for the wait time of response retransmissions. For INVITE, since an ACK could be lost, the UAS must wait at least 32 seconds (assuming the default transaction timer on other end is 32 seconds) to receive any retransmissions of responses from the UAS and send an ACK. In a Cisco BTS 10200 implementation, this transaction clearing timer is only applicable for INVITE requests. For non-INVITE, the transaction is cleared immediately upon receipt of final response
- TIMER-E-MILLI—The UAC timer for non-INVITE request retransmit interval. For example, if the value is 500 ms, the non-INVITE request retransmissions occurs at the interval of 500 ms, 1s, 2s, 4s, 4s, 4s, 4s, 4s, 4s, 4s (assuming TIMER-F-SECS defined below is 32 seconds and TIMER-T2-SECS defined above is 4 seconds).
- TIMER-F-SECS—The UAC non-INVITE transaction timer that limits the number of retransmissions for non-INVITE requests.
- TIMER-G-MILLI—The UAS timer implemented to achieve reliability of successful final responses to INVITE requests. It starts when using a reliable transport protocol such as TCP. Even though the transport protocol may be reliable up to the next hop, it is not guaranteed reliable end-to-end if there are several proxy servers along the path when setting up the call. This timer is started upon sending a final response for INVITE requests and determining the response retransmission interval. The timer stops when a matching ACK is received for the final response sent. For example, if a 200 OK is sent for INVITE, then the UAS must receive the matching ACK for the 200 OK. If the TIMER-G-MILLI is 500 ms, the final response to the INVITE from the UAS retransmits at the interval of 500 ms, 1s, 2s, 4s, 8s, 16s, 32s (assuming TIMER-H-SECS is 32 seconds).
- TIMER-H-SECS—The UAS timer responsible for clearing an incomplete INVITE UAS transaction. It also controls the number of INVITE final response retransmissions sent to UAC. The timer is started upon sending a final response for the INVITE request. It is the total wait time for ACK receipt from UAC.
- TIMER-I-SECS—This UAS timer is the wait time for ACK retransmits. It frees the server transaction resources, and starts when the first ACK to the final response is received for INVITE requests. Upon receipt of an ACK for certain INVITE final responses (401, 415, 420, 422, 423, 480 and 484), value of timer I is set to a fixed duration of 32 seconds. The responses result in resubmission of the original INVITE with modifications, and prevent the resources from prematurely freeing. A 481 (Call-Leg/Transaction does not exist) or a 408 (Request Timeout) response sent for the INVITE results in a much smaller fixed duration of four seconds for timer I. This ensures that CCB resources are promptly freed when the call is not set up, allowing reuse for other calls. For ACK to all other INVITE final responses, which are not typically followed by a re-attempt, the timer duration for this timer is set at TIMER-I-SECS.

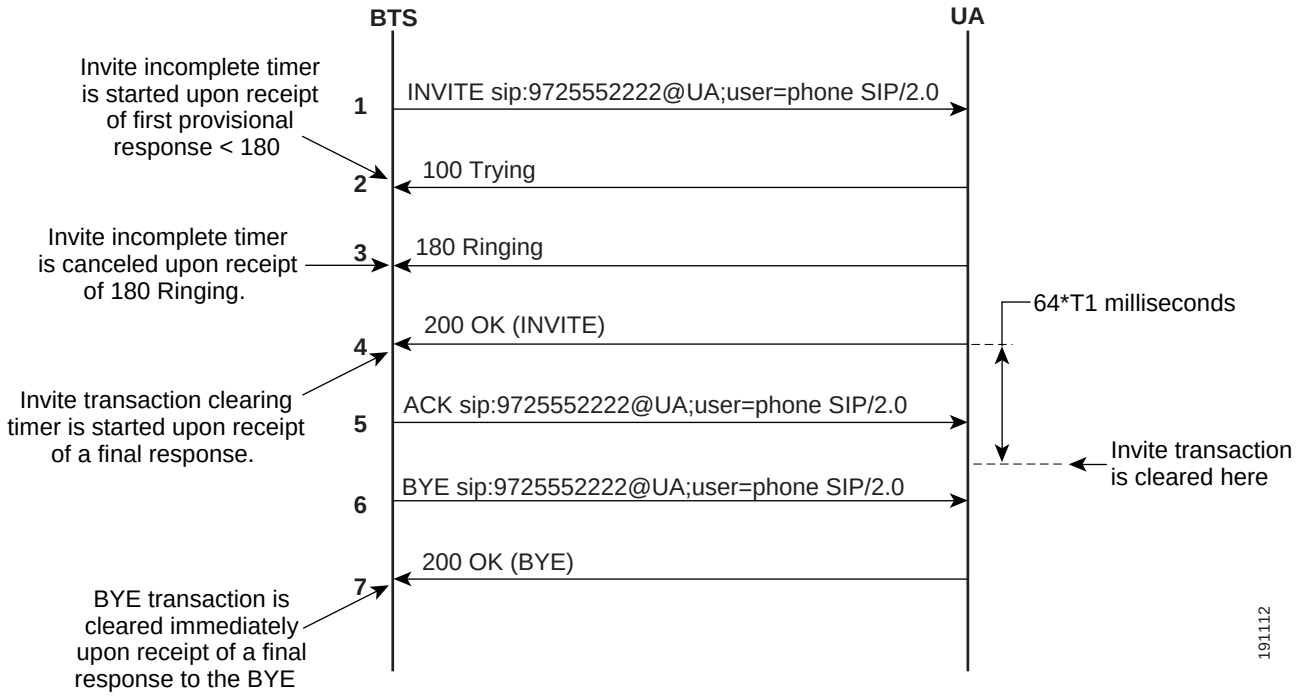
  When a BYE is subsequently sent or received on a call in progress, and timer I is running for that call, it is canceled and restarted for a smaller fixed duration of four seconds to reduce CCB hold time after call completion, and to optimize CCB resource usage.

- TIMER-J-SECS—This UAS timer cleans up non-INVITE UAS transactions. A shorter non-configurable timer of four seconds is used for BYE and CANCEL. Additionally, when a BYE or CANCEL is sent or received on a call in progress, if timer J is running for any non-INVITE transaction associated with that call, it is canceled and restarted for a smaller fixed duration of four seconds to reduce CCB hold time after call completion, and to optimize CCB resource usage.
- INVITE-INCOMPLETE-TIMER-SECS—This UAC timer cleans up UAC INVITE transactions for which a provisional response less than 180 was received, but no ringing or final response was received within a reasonable period of time. This timer starts upon receipt of the first provisional response (>=100 and <180) for the INVITE message sent. Upon receipt of the final response or 18x response to INVITE request, this timer is canceled.

  This timer is also started if a CANCEL is sent, to clean up the INVITE transaction in case of a final response (487), indicating that the request was canceled, is not received.

  The process involving receipt of the 180 response is shown in Figure 2-3.

Figure 2-3 Invite Incomplete Timer Process with 180 Response



- MIN-SE (session timer)—This specifies the minimum session-expires allowed on the Cisco BTS 10200. Any INVITE request received with a session-expires lower than the MIN-SE is rejected with a 422 response with a header Min-SE = MIN-SE.
- SESSION-EXPIRES-DELTA-SECS (session timer)—This cleans up resources in case of abnormal session end. The Cisco BTS 10200 sends the SESSION-EXPIRES-DELTA-SECS as the session-expires header in the initial INVITE. When a session is established, a session timer is started based on the negotiated value (it may be lower or equal to the SESSION-EXPIRES-DELTA-SECS). If Cisco BTS 10200 is determined as the refresher, then it starts a session timer for duration of half the negotiated time. A re-INVITE or update is sent out upon timer expiry to refresh the session. If the remote end is determined as the refresher, then a session timer is started for duration of (negotiated session-expires -10secs). In this case, a BYE is sent to end the session if a session refresh (re-INVITE/update) is not received within the expiry of session timer.

Note When the SESSION-EXPIRES-DELTA-SECS timer expires, the BTS 10200 might send a Re-Invite (as opposed to an Update) with the previously sent SDP. If the BTS 10200 receives a 200 OK with the SDP changed from the previously received SDP, the BTS 10200 does not send this changed SDP to the origination.

To provision these timers, see the SIP Timer Values section in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

Calculation of Timer Retransmission Count

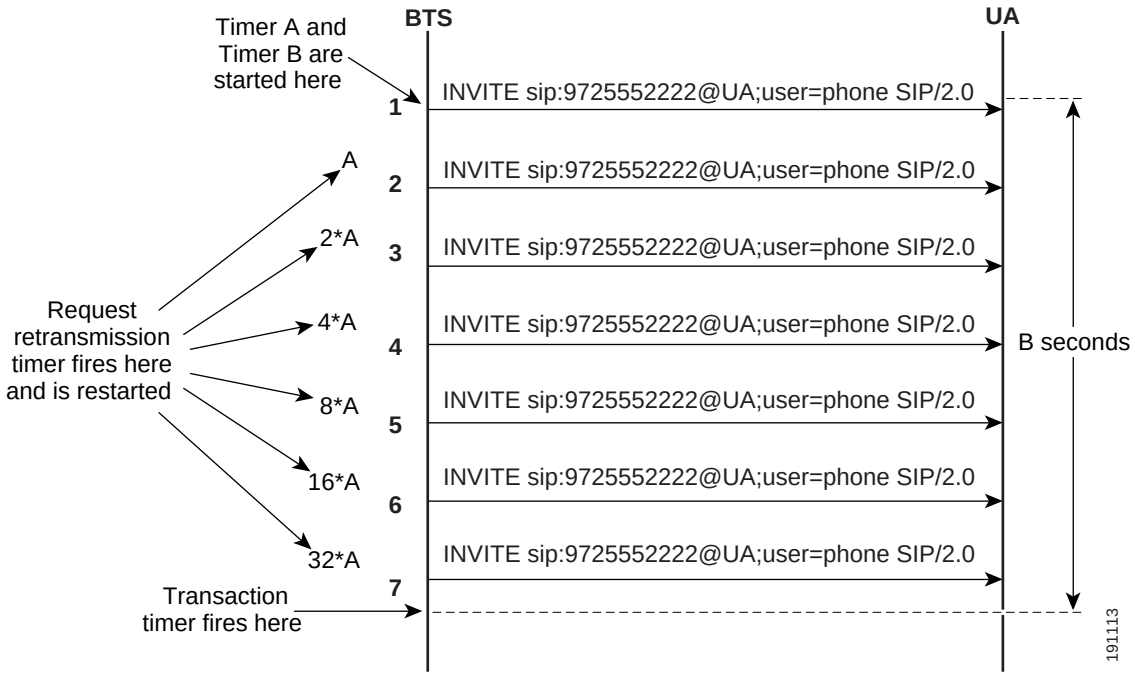
The retransmit count, or number of times the same request or response is retransmitted after the message is sent once to the transport layer, is computed based on RFC3261 recommendations.

INVITE Retransmit Count

If there is no response for the initial INVITE request, then INIVTE requests are retransmitted as shown:

For example, if TIMER-A-MILLI is 500 ms and TIMER-B-SECS is 32 seconds, then there are six retransmissions after the first request, for a total of seven requests from the UAC. The retransmissions occur at intervals of 500 ms, 1s, 2s, 4s, 8s, 16s, and 32s. The invite retransmission process is shown in Figure 2-4.

Figure 2-4 Invite Retransmissions with No Response



Non-INVITE Retransmit Count

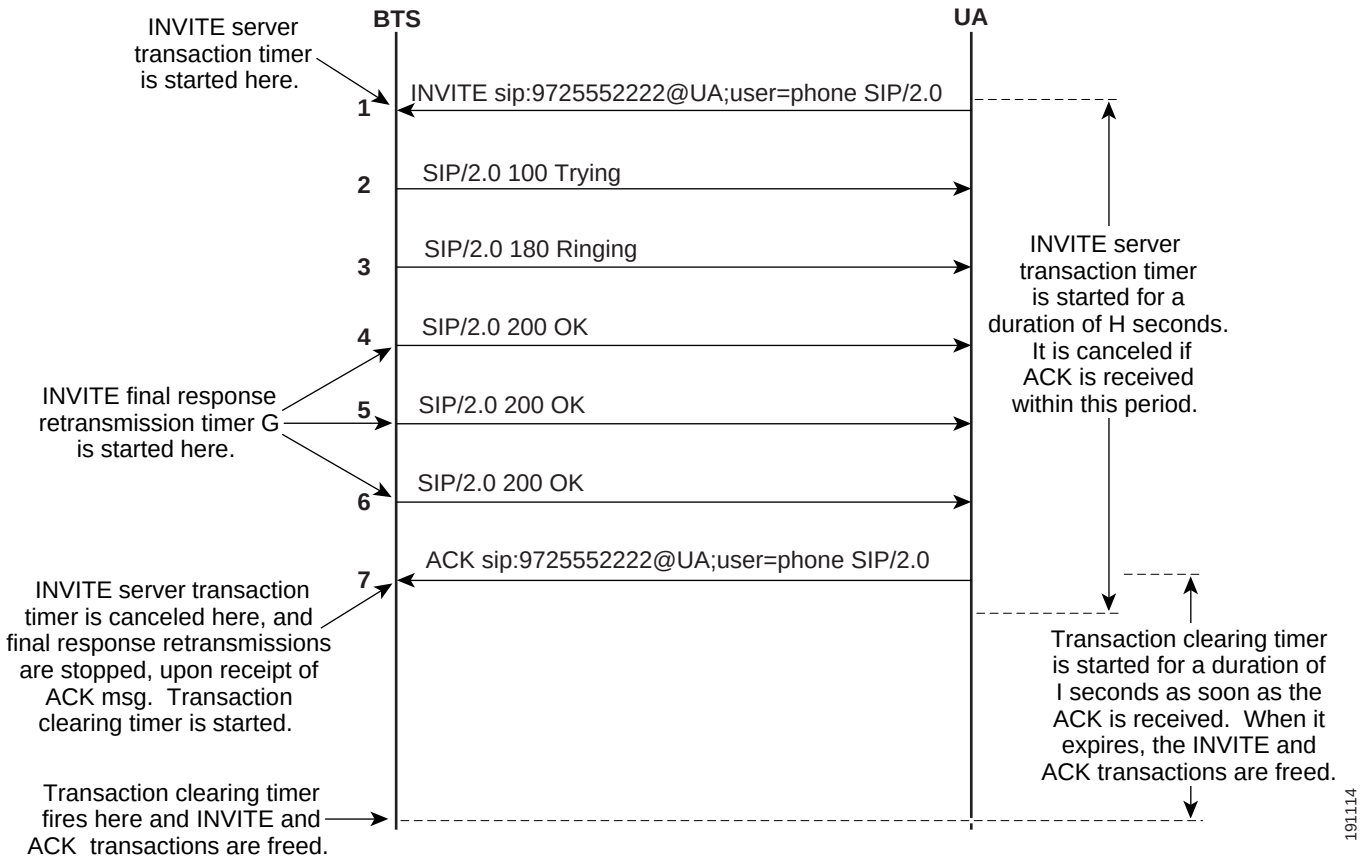
If there is no response for the initial non-INVITE request, then INIVTE requests are retransmitted as shown:

For example, if TIMER-E-MILLI is 500 ms, TIMER-T2-SECS is four seconds and TIMER-F-SECS is 32 seconds, then non-INVITE retransmissions occur at intervals of 500 ms, 1s, 2s, 4s, 4s, 4s, 4s, 4s, 4s, 4s. This means that retransmissions occur with an exponentially increasing interval that caps at T2. In this particular scenario, there are total 10 retransmissions which is a total of 11 requests from UAC.

Response Retransmit Count

If no ACK is received for the final response of the INVITE request, the responses are retransmitted. This process is shown in Figure 2-5.

Figure 2-5 Invite Server Transaction Timer Cancelled Upon Receipt of ACK



Reliable Provisional Responses

SIP defines two types of responses, provisional and final. Final responses convey the result of the request processing, and are sent reliably. Provisional responses provide progress information about the request processing, but are not sent reliably in the base SIP protocol. The reliable provisional responses feature provides end-to-end reliability of provisional responses for Cisco BTS 10200 SIP subscribers.

Provisional responses in SIP telephony calls represent backward alerting and progress signaling messages, which are important when interoperating with PSTN networks. Therefore, for SIP-T calls on the Cisco BTS 10200, reliable provisional responses are mandatory. They are optional for regular SIP calls.

Cisco BTS 10200 support for this feature follows the specifications described in RFC 3262. A provisioning flag is provided to enable or disable this feature, and is disabled by default. For SIP trunks provisioned as "SIP-T," the system internally ignores the flag and enables the feature always. In this case, the feature is mandatory. Therefore, the ability to enable or disable the feature applies to regular SIP trunks only. There is one exception: SIP-T trunks receiving SIP-T calls (calls with ISUP attachments) may also receive incoming regular SIP calls. In this case, the feature (enabled or disabled) for that regular SIP call is determined by the provisioning flag on that SIP-T trunk. The provisioning flag (PRACK_FLAG) is a member of the Softswitch Trunk Group profile. For provisioning details, see the *Cisco BTS 10200 Softswitch SIP Provisioning Guide*.

For calls received on a Cisco BTS 10200 regular SIP trunk, or regular SIP (non-SIP-T) calls received on a SIP-T trunk, the following feature behavior applies:

- If the received INVITE indicates this feature is required, all provisional responses are sent reliably, regardless of the provisioned feature setting on the trunk.
- If the received INVITE indicates this feature is supported, then all provisional responses are sent reliably if the feature is provisioned enabled on the trunk.
- If the received INVITE indicates the feature is not supported, the call is refused if the feature is enabled on the trunk.
- If the received INVITE indicates the feature is not supported, the call is accepted if the feature is disabled on the trunk. Provisional responses are not sent reliably.

For calls sent out a Cisco BTS 10200 regular SIP trunk, the following feature behavior applies:

- If the feature is provisioned enabled on the trunk, the SIP Invite message sent contains a 'Required' header with a tag value of '100rel.'
- If the feature is enabled on the trunk, and the remote endpoint supports or requires the feature, all provisional responses are sent reliably to Cisco BTS 10200.
- If the feature is enabled on the trunk, and the remote endpoint does not support the feature, the remote endpoint refuses the call.
- If the feature is disabled on the trunk, the SIP Invite message sent contains a 'Supported' header with a tag value of '100rel.'
- If the feature is disabled on the trunk, and the remote endpoint supports the feature, the remote endpoint controls which provisional response sent requires reliability.
- If the feature is disabled on the trunk, and the remote endpoint does not support the feature, provisional responses are not received reliably.

For SIP-T calls received on a Cisco BTS 10200 SIP trunk provisioned as SIP-T, the following feature behavior applies:

- If the received INVITE indicates this feature is required or supported, all provisional responses are sent reliably.
- If the received INVITE indicates the feature is not supported, the call is refused.
- For all calls sent out a Cisco BTS 10200 SIP trunk provisioned as SIP-T, the following feature behavior applies:
- The SIP-T Invite message sent contains a 'Required' header with a tag value of '100rel.'

- If the remote endpoint supports or requires the feature, all provisional responses are sent reliably to Cisco BTS 10200.
- If the remote endpoint does not support the feature, the remote endpoint refuses the call.

Text-GUI Features

Cisco BTS 10200 supports SIP client/handset text-based user interface (UI) provisioning for a select set of features. This is in contrast to numerous supplementary features supported natively by the SIP client/handset itself. Some of the features require updating the status on the network database. Cisco BTS 10200 provides complimentary support to SIP clients/handsets to update end user feature access status on the switch network database.

Provisioning in this context refers to feature activation or deactivation, and setting any applicable Directory Numbers (DNs) associated with the feature. If a SIP handset is used, the phone's LCD panel is used as a menu display area to guide the user toward feature provisioning. If a SIP software client is used, the UI display region in the client software is used to guide the user through feature provisioning.

There may be multiple lines on the SIP phone, but currently services configured using softkeys on the phone are only available to one of those lines. The subscriber for that line is provisioned by Cisco BTS 10200 with the MAC address of the phone (see "MAC to Subscriber" section on page 5-32).

Supported Handsets

Cisco BTS 10200 supports any SIP client/handset that supports CallManager XML 3.0.

Supported Features

The following features have SIP client/handset based provisioning support:

- Call forwarding unconditional activation (CFUA), call forwarding unconditional deactivation (CFUD)
- Call forwarding on busy variable activation (CFBVA), Call forwarding on busy variable deactivation (CFBVD)
- Call forwarding on no answer variable activation (CFNAVA), call forwarding on no answer variable deactivation (CFNAVD)
- Do Not Disturb activation (DND-ACT), Do Not Disturb deactivation (DND-DEACT)
- Anonymous call rejection activation (ACR-ACT), anonymous call rejection deactivation (ACR-DEACT)

Accessing Features

The following sections describe how to access the features.

SIP Handset

The SIP handset provides a button labeled "Services" or an icon suggesting "Services." Initial access to feature provisioning is through the "Services" button. After initial access, the UI display area provides a menu-driven interface, and follows a menu depending on the feature type selected.

Navigating the menu is accomplished using the “Up” and “Down” arrow buttons or via menu numbers. At any level of navigation, use the “Exit” softkey to go back one step in the menu hierarchy. Select menu items using the “Select” softkey button. The numeric dial is used to enter DN information.

Menu Hierarchy

Feature Options
- Call Forwarding
  - Call-Fwd Busy
    - Activate/Deactivate Feature
    - Set/Change Forwarding Number
    - Number:
  - Call-Fwd Unconditional
    - Activate/Deactivate Feature
    - Set/Change Forwarding Number
    - Number:
  - Call-Fwd No Answer
    - Activate/Deactivate Feature
    - Set/Change Forwarding Number
    - Number:
    - Anonymous Call Rejection
  - Activate/Deactivate Feature
- Do Not Disturb
  - Activate/Deactivate Feature

SIP Software Clients

The user interface for applicable software clients is similar to a SIP handset.

Call Transfer (Blind and Attended)

The SIP call transfer (CT) feature is supported for SIP subscribers on Cisco BTS 10200 Release 4.5.x. Call transfer in Cisco BTS 10200 requires provisioning the “REFER” feature as an office trigger. See the *Cisco BTS 10200 SIP Protocol Provisioning Guide* for details.

The call transfer feature requires phone support for sending the SIP REFER message. See the phone documentation for details on the user interface and procedures to effect a call transfer. Both blind and attended transfers are supported.

The following caveats apply when using call transfers:

1. Attended transfer to a transfer-target is supported only after the target answers; that is, consultative attended transfer is supported. Attended transfer is not possible, while the transfer-target is being alerted (ringing state).

2. Only calls on Cisco BTS 10200 may be replaced by an attended transfer. If a SIP subscriber has independently placed a call to another SIP subscriber, without using Cisco BTS 10200, then Cisco BTS 10200 cannot replace the call made outside of Cisco BTS 10200.

Distinctive Ringing

Distinctive ringing uses a special ringing pattern to alert the called user of incoming calls from pre-selected telephone numbers. This is a CLASS feature and is offered to both Business and Residential users.

You can edit the list of selected numbers though the Screening List Editing (SLE) feature, which requires configuring an IVR with the Cisco BTS 10200 Softswitch. Distinctive ringing can be assigned to a station and to the group, and applied to users based on the call type/calling number. When assigned to a group, distinctive ringing is applied to users in the group based on the call type. When assigned to the line, distinctive ringing is applied to the user based on the calling number. The Cisco BTS 10200 sends an Alert-Info header in the outgoing INVITE message, instructing the SIP phone to play a specific ring tone.

Distinctive ringing depends on the SIP phone's capability to support processing of the information received in Alert-Info header.

Distinctive Ringing for Centrex DID Calls

The Cisco BTS 10200 Softswitch sends an Alert-Info header in the outgoing INVITE message, instructing the SIP phone to play a specific ring tone. Distinctive ringing depends on the SIP phone's capability to support processing the information received in Alert-Info header.

Diversion Indication

Diversion indication provides supplemental redirection information to the SIP entity receiving the call. The SIP entity uses this information to identify from whom the call was diverted, and why the call was diverted. It also provides information for each redirection if multiple redirections occurred. This is provided in the form of a SIP 'Diversion:' header.

Forwarding information allows applications such as SIP voice-mail servers to access the mailbox of the original called party for proper outgoing greeting and message deposit when a forwarded call is received. Billing systems also use the information to determine the charged party of the call where it is the last forwarding party that is billed.

The BTS 10200 supports this feature following the specifications described in the IETF draft draft-levy-sip-diversion-02.txt. For incoming calls, Cisco BTS 10200 uses the party number information from the top-most and bottom-most diversion headers. The Cisco BTS 10200 reads the diversion counter, across all diversion headers to determine the total diversion count. For outgoing calls, The BTS 10200 sends 0, 1 or 2 diversion headers, depending on the forwarding information of the call.

Diversion header parameters support is limited to the diversion 'counter' and the diversion 'reason.' These two parameters in diversion headers are populated for outgoing calls and interpreted on incoming calls.

For INVITEs sent out by the BTS 10200, the following behavior applies:

- If no diversion information is available, no diversion headers are included.

- If there is an ‘original called’ party, one diversion header is added to the outgoing INVITE message.
- If there is a ‘last forwarding’ party, a second diversion header is added on top of the original called party diversion header.
- Each outgoing diversion header is populated with the party number, the diversion reason and diversion count.
- For Release 4.5.1, Maintenance Release 2 and later—Privacy parameters are sent and received in the Diversion header.
- For Release 4.5.1, Maintenance Release 2 and later—If the original called number (OCN) and/or the redirected DN (RDN) are being sent in Diversion headers towards local SIP subscribers, and the presentation value is not allowed, the system applies anonymous to them as follows:
  - If an original called number (OCN) exists, it populates the URL as anonymous@anonymous.invalid in the To header.
  - If a Diversion header is added, it populates the ‘user’ part of the diversion header with ‘anonymous.’