C H A P T E R 2

SIP Subscribers

Revised: April 17, 2008, OL-12397-13

The Cisco BTS 10200 Softswitch supports SIP subscribers on SIP phones that are compliant with RFC 3261 or RFC 2543. This section describes the support for SIP subscribers and how to provision SIP subscriber features.

In this document

- SIP subscriber means a SIP phone that is registered directly to the BTS 10200 and for which the BTS 10200 maintains subscriber information.

- SIP ANI-based subscriber means a SIP phone that communicates with the BTS 10200 over a SIP trunk.

Note For quick-reference tables listing the subscriber features, see the "Comparison of SIP-Based Features and MGCP-Based Features" section on page 2-13.

This section covers the following topics:

SIP Phone Initialization

Figure 2-1 shows an example of SIP phone initialization on bootup, that is, how a typical phone might initialize itself and establish its identity with the BTS 10200.

The image shows actions that occur external to the BTS 10200—It does not show how the BTS 10200 controls SIP initialization. Instead, it shows how a client can establish its identity with the BTS 10200.

The circled numbers in the image indicate the numerical order in which the sequence occurs.

Figure 2-1   *Example of SIP Phone Initialization*
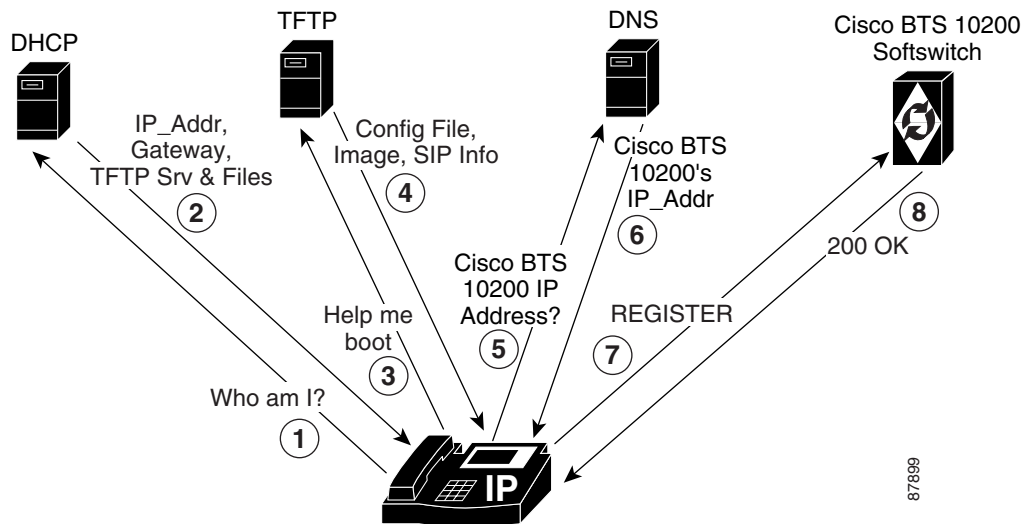
Provisioning a SIP Subscriber

To provision a SIP subscriber, see the "SIP Subscriber Provisioning" chapter in the *Provisioning Guide*.

SIP Registration and Security

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

Note   Third-party registration is not supported.

It is possible to register multiple contacts for a single AOR; however, if multiple contacts are registered for a single subscriber, the 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 BTS 10200 challenges the SIP subscriber based on provisioning in the Serving Domain Name table. If the Serving Domain Name table indicates that authentication is required, the BTS 10200 challenges the SIP request (Register/INVITE) according to the authentication procedures specified in the SIP Protocol RFC 3261. If the BTS 10200 receives valid credentials, the authenticated AOR from the User Authorization table identifies the subscriber based on the Address of Record to Subscriber table. (For specific provisioning parameters, see the applicable tables in the Cisco BTS 10200 Softswitch CLI Database.)

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

The registration data is replicated on the standby BTS 10200. The 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 BTS 10200 generates a warning event when a request from a client fails authentication. This can indicate a provisioning error or an attempt by an unauthorized client to communicate with the BTS 10200.

The contacts registered for an AOR can 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

SIP Registration ensures that a SIP REGISTER message to the 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.

Description

Prior to Release 4.5.1, SIP endpoint registration was based on 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 BTS 10200 can indicate SECURE_FQDN provisioning for specified SIP term-type subscribers. This indication consists of specifying an FQDN with the subscriber AOR. The FQDN is the address/location of the SIP endpoint and is added to the AOR table. The FQDN does 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.

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

- One and only one AOR is associated with 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 presents a case in which a VoIP subscriber (Subscriber 1) uses the 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 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

This section shows the CLI commands you need to provision a secure fully qualified domain name (FQDN) of a SIP endpoint.

Note Use this procedure to provision subscribers on the BTS 10200. The procedure does not cover the security of configuration files provisioned on the SIP adapter (for example, an ATA), which are the responsibility of the service provider.

The SECURE_FQDN token is present in both 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 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. To add AOR2SUB records, you must specify specify the AOR ID on a subscriber record.

Provision a New SIP Subscriber

Step 1 To provision a new SIP subscriber with the secure FQDN feature, enter the following command.

> **Note** This command automatically adds a corresponding entry in the AOR2SUB table.

```
add subscriber id=sub1; sub-profile-id=subpf1; category=individual;
dn1=241-555-1018; term-type=SIP; aor-id=<aor-id of SIP adapter port for sub1>;
secure-fqdn=<secure-fqdn of the SIP adapter>;
```

Step 2 (Optional) To provision an additional subscriber on the same SIP adapter, enter the following command:

```
add subscriber id=sub2; sub-profile-id=subpf1; category=individual;
dn1=241-555-1022; term-type=SIP; aor-id=<aor-id of SIP adapter port for sub2>;
secure-fqdn=<secure-fqdn of the SIP adapter>;
```

> **Note** If there are multiple subscribers on a single SIP adapter (such as an ATA), these subscribers might share the same IP address. Therefore, you can provision all of these subscriber records with a single secure-fqdn, and in the DNS, this FQDN can point to the applicable IP address. The id, dn1, and aor-id tokens must have unique values for each subscriber.

Enable or Disable Secure FQDN for an Existing Subscriber

To enable or disable the secure FQDN feature for a successfully registered subscriber, enter the following commands:

Step 1 Take the AOR out of service (OOS). This command removes all registered contact.

```
change aor2sub aor-id=241-555-1018@sia-SYS41CA146.ipclab.cisco.com; status=oos;
```

Step 2 To enable the secure FQDN feature for an existing subscriber, enter the following command:

```
change subscriber id=sub1; secure-fqdn=ata-SYS41CA146.ipclab.cisco.com
```

To disable the secure FQDN feature for an existing subscriber, enter

```
change subscriber id=sub1; secure-fqdn=null
```

> **Note** If secure-fqdn is not provisioned for the subscriber, the system does not provide the secure FQDN feature to that subscriber. If secure-fqdn has previously been provisioned for the subscriber, setting secure-fqdn to null disables the feature.

Step 3 To bring the AOR back in service (INS), enter the following command:

```
change aor2sub aor-id=241-555-1018@sia-SYS41CA146.ipclab.cisco.com; status=ins;
```

Step 4   Reboot the adapter device (such as ATA) for this subscriber.

Operations

The system performs the following checks. 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 endpoints are not allowed.

Cisco BTS 10200 Challenges Registration

On receiving a REGISTER message from a secure-provision SIP endpoint, the 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 are 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 the 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 2-6 occurs before any new calls are accepted.

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

When a call originates from or terminates to a secure-provision SIP endpoint

1. The system 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 must be 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 second item in this list.

Call Processing

The SIP application in the 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, that comes 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 there is no DNS resolution, 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 the address is incorrect, a 500 Internal Server Error response is returned.

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

    If the address is not identical, a 403 Forbidden response is returned.

5. If the Request is a Register, it is verified to have a single Contact header.

    If there is not a single contact header, a 403 Forbidden response is returned.

6. If the SIP request is an initial INVITE (including an INVITE resubmitted with credentials), it is verified that there is an unexpired registered contact for the AOR.

    If here is not an unexpired registered contact, 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 it does not yield the proper address, 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 the addresses are not identical, 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 to be 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 to be identical with the IP address of the Secure-IP1.

    If the addresses are not identical, the response is dropped. This has the same result as the non-receipt of that response, such as would happen with 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 the address does not resolve properly, the response is dropped. This has the same result as the non-receipt of that response, such as would happen with a call failure.

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

Rules for Sending a SIP INVITE Message from the 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

The following TMM counters are supported for secure FQDN violations:

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

Note For a full list of measurements, see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

Events and Alarms

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

Type: SECURITY(6)

DESCRIPTION: Secure SIP Endpoint Validation Failure

SEVERITY: WARNING

Note For a full list of events and alarms, see the *Cisco BTS 10200 Softswitch Troubleshooting Guide*.

SIP User Authentication

The BTS 10200 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, because 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 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 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 tables affect authentication for SIP subscribers:

- AOR

- Serving Domain

- Auth-Realm

- User-Auth

See the *Cisco BTS 10200 Softswitch CLI Database* for more information about the tables.

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

Figure 2-2   Authentication and Processing of an Incoming Request (for Example, INVITE)
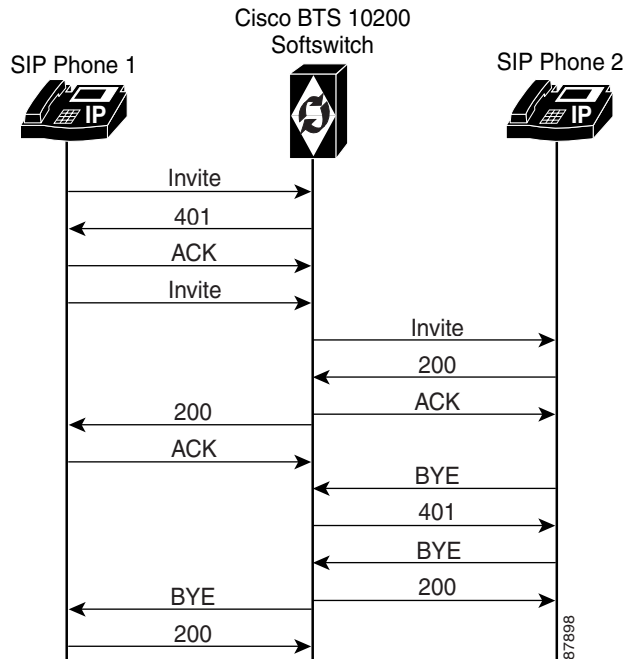
The BTS 10200 validates the hostname of the ReqUri of every incoming SIP request against the list of names provisioned in the Serving-Domain-Name table. The BTS 10200 hostname used by devices (in the ReqUri), when they send requests to the BTS 10200, should be provisioned in the Serving-Domain-Name table 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 Authorization table in the *Cisco BTS 10200 Softswitch CLI Database*.

SIP Subscriber Calls

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

The system allows SIP subscribers to call other SIP subscribers or SIP trunks connected to the BTS 10200. The provisioned dial plan determines whom a subscriber can call. A SIP subscriber can receive a call as long as the subscription's registration is current, or a static registration has been provisioned.

Provisioning Session Timers for SIP Subscribers

The system uses session timers to periodically refresh SIP sessions during call processing or in-progress calls. You can enable or disable session timers for calls to and from all SIP subscribers on the BTS 10200 through the SUB_SESSION_TIMER_ALLOWED parameter in the ca-config table. They are disabled by default.

Use the commands in this section to provision session timers for SIP subscribers. Session timer defaults for subscribers are defined by internal defaults. They can be adjusted through the commands shown in this section.

Note   For a detailed description of session timers, see "SIP Session Timers" section on page 4-7

Step 1   Adjust the session timer values in the sip-timer-profile table.

Note   The session duration field value is in seconds with a range of 100 to 7200.
The minimum session duration field value is in seconds with a range of 100 to 1800.

We recommend a value of at least 1800 for each of these fields.

```
add sip_timer_profile id=<timer_profile_id>; session_expires_delta_secs=7200;
min-se=1800;
```

Step 2   Enable session timers for SIP subscribers:

```
add ca-config type=SUB_SESSION_TIMER_ALLOWED; datatype=BOOLEAN; value=Y;
```

Step 3   If not already done, add a default sip-timer-profile-id to the ca-config table:

```
add ca_config type=SIP_TIMER_PROFILE_ID; datatype=STRING;
value=<sip_timer_profile_id>;
```

SIP Timer Values for SIP Subscribers

Note   This section describes how to provision SIP timer values for SIP subscribers. For a comprehensive listing of SIP timers, see Chapter 4, "SIP System Features."

You can customize SIP timers through the sip-timer-profile table. A record in this table can then be configured to apply to all subscribers switch-wide. The system operates with default SIP protocol timer values, as noted in the SIP specification. These default values are adequate for many installations. If customization is required, a sip-timer-profile table can be provisioned and associated with all calls.

Use the following steps to provision the SIP timer values.

Step 1   Adjust the SIP timer values in the sip-timer-profile table if necessary (example shown).

```
add sip-timer-profile id=<timer_profile_id>; timer-t1-milli=500;
```

Step 2   If not already done, add a default sip-timer-profile-id to the ca-config table:

```
add ca-config type=sip_timer_profile_id; datatype=string;
value=<sip_timer_profile_id>;
```

Diversion Indication for SIP Subscribers

Diversion indication provides supplemental redirection information to the SIP entity receiving a 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 the Diversion Indication feature according to the specifications in the IETF document draft-levy-sip-diversion-02.txt. For incoming calls, the BTS 10200 uses the party number information from the top-most and bottom-most diversion headers. The BTS 10200 reads the diversion count 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 parameter 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 the diversion count.
- For Release 5.0, Maintenance Release 1 and later, privacy parameters are sent and received in the Diversion header.
- For Release 5.0, Maintenance Release 1 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 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.

Comparison of SIP-Based Features and MGCP-Based Features

Table 2-1 lists the MGCP features available (in the Feature column) and then describes how the feature differs when it is used as a SIP feature.

Table 2-1   MGCP Features and SIP Support

MGCP-Based Feature	Abbreviation	Support for SIP Phone Compared to Support for MGCP-Based Phone
8XX Toll-Free	8xx	Same as MGCP.
911 Emergency-Service	911	Only E911 support (without the suspend procedure for 45 minutes). Basic 911 with suspend procedure is not supported.
		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.
		The Public Safety Answering Point (PSAP) is selected based on default user location. No mobility is supported.
Anonymous Call Rejection	ACR	Same as MGCP, when provided by the BTS 10200. Also provided by the phone.
Anonymous Call Rejection Activation	ACR_ACT	BTS 10200 functionality is same for SIP subscribers as for MGCP.
		ACR_ACT is also supported on some SIP phones. Depending on the specific phone, the feature on the BTS 10200 might work jointly with the feature on the phone.
Anonymous Call Rejection Deactivation	ACR_DEACT	BTS 10200 functionality is same for SIP subscribers as for MGCP.
		ACR_DEACT is also supported on some SIP phones. Depending on the specific phone, the feature on the BTS 10200 might work jointly with the feature on the phone.
Automatic Callback	AC	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Automatic Callback Activation	AC_ACT	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Automatic Callback Deactivation	AC_DEACT	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Automatic Recall	AR	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Automatic Recall Activation	AR_ACT	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Automatic Recall Deactivation	AR_DEACT	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Busy Line Verification	BLV	Not supported.
CALEA and LI	n/a	For information on lawful intercept (LI) and CALEA, see the "Lawful Intercept and Enhanced CALEA" chapter in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions*.
Call Block	CBLK	Same as MGCP.

Table 2-1   MGCP Features and SIP Support (continued)

MGCP-Based Feature	Abbreviation	Support for SIP Phone Compared to Support for MGCP-Based Phone
Call Forward Busy [1]	CFB	Same as MGCP.
Call Forward Busy Variable Activation	CFBVA	Single-stage digit collection.
Call Forward Busy Variable Deactivation	CFBVD	Same as MGCP.
Call Forward Busy Interrogation	CFBI	Single-stage digit collection.
Call Forward Combined [1]	CFC	Same as MGCP.
Call Forward Combined Activation	CFC_ACT	Single-stage digit collection.
Call Forward Combined Deactivation	CFC_DEACT	Same as MGCP.
Call Forward No Answer [1]	CFNA	Same as MGCP.
Call Forward No Answer Variable Deactivation	CFNAVA	Single-stage digit collection.
Call Forward No Answer Variable Deactivation	CFNAVD	Same as MGCP.
Call Forward No Answer Interrogation	CFNAI	Single-stage digit collection.
Call Forward Unconditional [1]	CFU	Same as MGCP.
Call Forward Unconditional Activation	CFUA	Single-stage digit collection.
Call Forward Unconditional Deactivation	CFUD	Same as MGCP.
Call Forward Unconditional Interrogation	CFUI	Single-stage digit collection.
Call Hold	CHD	Functionality provided by the phone. The BTS 10200 supports the interface.
Call Park	CPRK	Not supported.
Call Park and Retrieve	CPRK_RET	Not supported.
Call Transfer	CT	For SIP phones, this feature is provided as part of REFER support on the BTS 10200. See the "Call Transfer (Blind and Attended) with REFER" section on page 2-31 for details.
Call Waiting	CW	Functionality provided by the phone. The BTS 10200 supports the interface.
Call Waiting Deluxe	CWD	Varies with phone functionality.
Call Waiting Deluxe Activation	CWDA	Varies with phone functionality.
Call Waiting Deluxe Deactivation	CWDD	Varies with phone functionality.

Table 2-1   MGCP Features and SIP Support (continued)

MGCP-Based Feature	Abbreviation	Support for SIP Phone Compared to Support for MGCP-Based Phone
Call Waiting Deluxe Interrogation	CWDI	Varies with phone functionality.
Calling Identity Delivery and Suppression (Delivery) [2]	CIDSD	Presentation status from the phone, and single-stage digit collection.
Calling Identity Delivery and Suppression (Suppression) [2]	CIDSS	Presentation status from the phone, and single-stage digit collection.
Calling Identity Delivery on Call Waiting	CIDCW	Functionality provided by the phone. Cisco BTS 10200 supports the interface.
Calling Name Delivery [3]	CNAM	Same as MGCP.
Calling Name Delivery Blocking	CNAB	Presentation status from the phone, and single-stage digit collection.
Calling Number Delivery [3]	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.
Calling Number Delivery Blocking	CNDB	Presentation status from the phone, and single-stage digit collection.
Cancel Call Waiting	CCW	Functionality provided by the phone. Cisco BTS 10200 supports the interface.
Class of Service	COS	CoS Screening supported, without Auth/Account code collection.
Custom-Dial-Plan	CDP	Same as MGCP.
Customer Originated Trace	COT	Same as MGCP.
Directed Call Pickup without Barge-in	DPN	Not supported.
Directed Call Pickup with Barge-in	DPU	Not supported.
Distinctive Alerting Call Waiting Indication	DACWI	This feature is provided to Centrex users only. Provisioning for SIP does not differ from provisioning for MGCP. However, the delivery method for DACWI is different. The Centrex administrator provisions a list of DNs that are to receive DACWI tones. In MGCP, the phone plays the tone specified by the BTS 10200 in the protocol message. In SIP, the tone provisioned for the DN is specified by the BTS 10200 in the Alert-Info header of the INVITE as a file URL. A SIP phone, if capable, interprets this header and plays the specified distinctive ringing or call-waiting tone.

Table 2-1   *MGCP Features and SIP Support (continued)*

MGCP-Based Feature	Abbreviation	Support for SIP Phone Compared to Support for MGCP-Based Phone
Distinctive Ringing Call Waiting	DRCW	Provisioning for SIP does not differ from provisioning for MGCP. However, the delivery method for DRCW is different. The subscriber provisions a list of DNs to receive DRCW tones. In MGCP, the phone plays the tone specified by the Cisco BTS 10200 in the protocol message. In SIP, the tone provisioned for the DN is specified by the Cisco BTS 10200 in the Alert-Info header of the INVITE as a file URL. A SIP phone, if capable, can interpret this header and play the specified distinctive ringing or call-waiting tone.
Distinctive Ringing Call Waiting	DRCW_ACT	Same as MGCP.
Do Not Disturb	DND	Same as MGCP, except that the reminder ring cannot be used with SIP devices. For additional information on DND, see the "Do Not Disturb" section on page 2-22.
Do Not Disturb Activation	DND_ACT	Same as MGCP.
Do Not Disturb Deactivation	DND_DEACT	Same as MGCP.
Group Speed Call—1 digit	GSC1D	Not supported.
Group Speed Call—2 digit	GSC2D	Not supported.
Hotline	HOTLINE	Not supported.
Hotline Variable	HOTV	Not supported.
Hotline Variable Activation	HOTVA	Not supported.
Hotline Variable Deactivation	HOTVD	Not supported.
Hotline Variable Interrogation	HOTVI	Not supported.
Incoming Simulated Facility Group	ISFG	Same as MGCP.
Local Number Portability	LNP	Same as MGCP.
Multiline Hunt Group	MLHG	MLHG is not supported for SIP subscribers.
Multiple Directory Number	MDN	Provisioning for SIP does not differ from provisioning for MGCP. However, the delivery methods for distinctive -ringing (a distinctive ring tone for each line of the MDN subscriber), and the distinctive tone on call waiting are different. You provision distinctive ringing and call waiting tones for each DN of the MDN subscriber in the same manner for MGCP and SIP. In MGCP, the phone plays the tone specified by the Cisco BTS 10200 in the protocol message. In SIP, the tone provisioned for the DN is specified by the Cisco BTS 10200 in the Alert-Info header of the INVITE as a file URL. A SIP phone, if capable, can interpret this header and play the specified distinctive ringing or call waiting tone.
Outgoing Call Barring	OCB	Same as MGCP.

Table 2-1   MGCP Features and SIP Support (continued)

MGCP-Based Feature	Abbreviation	Support for SIP Phone Compared to Support for MGCP-Based Phone
Outgoing Call Barring Activation	OCBA	Single stage digit collection.
Outgoing Call Barring Deactivation	OCBD	Single stage digit collection.
Outgoing Call Barring Interrogation	OCBI	Single stage digit collection.
Outgoing Simulated Facility Group	OSFG	Same as MGCP.
Remote Activation of Call Forwarding	RACF	Same as MGCP.
Remote Activation of Call Forwarding PIN	RACF_PIN	Same as MGCP.
Refer	REFER	This is not for MGCP users. Cisco BTS 10200 supports the SIP REFER interface to enable services such as Call-Transfer (attended, unattended) provided by the phone.
Selective Call Acceptance	SCA	Same as MGCP.
Selective Call Acceptance Activation	SCA_ACT	Same as MGCP.
Selective Call Forwarding	SCF	Same as MGCP.
Selective Call Forwarding Activation	SCF_ACT	Same as MGCP.
Selective Call Rejection	SCR	Same as MGCP.
Selective Call Rejection Activation	SCR_ACT	Same as MGCP.
Speed Call—1 digit	SC1D	Not supported.
Speed Call Activation—1 digit	SC1D_ACT	Not supported.
Speed Call—2 digit	SC2D	Not supported.
Speed Call Activation—2 digit	SC2D_ACT	Not supported.
Three-Way Calling	TWC	Functionality provided by the phone. The BTS 10200 supports the interface.
Three-Way Call Deluxe	TWCD	Varies with phone functionality.
Usage-Sensitive Three-Way Calling	USTWC	Functionality provided by the phone. The BTS 10200 supports the interface.
Warmline	WARMLINE	Not supported.

1. See additional information on call forwarding features in the "Call Forwarding" section on page 2-19.

2. See additional information on the delivery and suppression feature in the "Caller ID Delivery Suppression" section on page 2-21.

3. See additional information on calling name and calling number in the "Calling Name and Number Delivery" section on page 2-20.

Cisco BTS 10200 Softswitch-Based Features

Softswitch-based features are directly provided by the BTS 10200. SIP phones can 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 BTS 10200.

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

Summary

Table 2-2 lists the most commonly used Softswitch-based features; however, it is not an exhaustive list.

Note   The sections that follow the table provide additional details on selected softswitch-based features.

s

Table 2-2   BTS 10200-Based SIP Features

SIP Feature	Acronym
Activation and Deactivation of Anonymous Call Rejection	ACR
Anonymous Call Rejection Activation	ACR_ACT
Anonymous Call Rejection Deactivation	ACR_DEACT
Call Forwarding	CF
Call Forwarding on Busy Variable Activation	CFBVA
Call Forwarding on Busy Variable Deactivation	CFBVD
Call Forwarding on Busy Interrogation	CFBI
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 Unconditional Activation	CFUA
Call Forwarding Unconditional Deactivation	CFUD
Call Forwarding Unconditional Interrogation	CFUI
Call Waiting Deluxe Activation	CWDA
Call Waiting Deluxe Deactivation	CWDD
Call Waiting Deluxe Interrogation	CWDI
Called Party Termination	CPT
Caller ID Suppression	CIDS
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

Table 2-2   BTS 10200-Based SIP Features (continued)

SIP Feature	Acronym
Calling Name and Number Delivery	CND
Customer Access Treatment	CAT
Customer-Originated Trace	COT
Differentiated Services Code Point	DSCP
Direct Inward Dialing	DID
Direct Outward Dialing	DOD
Do Not Disturb	DND
Do Not Disturb Activation	DND_ACT
Do Not Disturb Deactivation	DND_DEACT
Emergency Call	E911
E.164 and Centrex Dialing Plan (Extension Dialing)	E.164
Incoming and Outgoing Simulated Facility Group	ISFG and OSFG
Multiple Directory Numbers	MDN
Operator Services (0-, 0+, 01+, 00 calls)	—
Outgoing Call Barring	OCB
Outgoing Call Barring Activation	OCBA
Outgoing Call Barring Deactivation	OCBD
Outgoing Call Barring Interrogation	OCBI
Remote Activation of Call Forwarding	RACF
Vertical Service Codes	VSC

Call Forwarding

The differences between the feature for SIP and the feature for MGCP are as follows:

- There is no tone provided for SIP users to prompt for forwarding digits. The SIP users enter the forwarding digits immediately after the VSC. This is called single-stage dialing.

- There is no dial tone played after the SIP user successfully activates or deactivates the Forwarding features. The SIP user always hears an announcement (if announcements are provisioned) or a re-order tone.

Call Forwarding Activation and Deactivation

Activation and deactivation of call forwarding features use the vertical service code (VSC), also known as a star code.

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 address of record (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

Activation and deactivation are accomplished using single-stage dialing.

Detailed Provisioning Procedure and Feature Description

Additional information on this feature is provided at the following links.

Provisioning Procedure	Feature Behavior (Feature Description and Handset Provisioning)
Call forwarding sections in the *Cisco BTS 10200 Softswitch Provisioning Guide*	"Call Forwarding Features" section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document

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 inserted 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 inserted 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.

Additional information on this feature is provided at the following links.

Provisioning Procedure	Feature Behavior (Feature Description and Handset Provisioning)
CND, CNAM, CNDB, and CNAB sections in the *Cisco BTS 10200 Softswitch Provisioning Guide*	"Calling Identity Features" section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document

Caller ID Delivery Suppression

The treatment for caller's identity is based on the presence of "anonymous" in the Display-Name field of the From header in the INVITE message. If the caller's identity is restricted in the incoming SIP INVITE message, the presentation is suppressed.

Caller Identity presentation (allowed/restricted) information for SIP subscribers is not maintained in the the BTS 10200 database. This information is maintained on the individual phones and can be provisioned through the phone softkeys. Permanent restriction on the phone can be overridden if the caller dials a feature (*) code on a per-call basis. This is a single-stage dialing for SIP subscribers.

Additional information on this feature is provided at the following links.

Provisioning Procedure	Feature Behavior (Feature Description and Handset Provisioning)
"CND, CNAM, CNDB, and CNAB" sections in the *Cisco BTS 10200 Softswitch Provisioning Guide*	"Calling Identity Delivery and Suppression (CIDSD and CIDSS)" section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document

Customer Access Treatment

Provisioning this feature for SIP is the same as provisioning it for MGCP. The provisioning commands for this feature are shown in Chapter 8, "Centrex Provisioning," in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Direct Inward Dialing

Provisioning this feature for SIP is the same as provisioning it for MGCP.

Assign the DID number to the subscriber as DN1 in the Subscriber table.

For information about the operation of this feature, 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 (a number 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 BTS 10200 along with the DDD number in the INVITE message. Secondary dial-tone capability is dependent on the SIP device used.

For information about the operation of this feature, see the DOD for PBX section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide.

Do Not Disturb

The Do Not Disturb (DND) feature enables a user to block incoming calls to the station on which the feature is activated. If no call forwarding features are activated, calls to the station are routed to busy treatment. This feature should be provisioned and activated on the BTS 10200 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 is a confirmation tone and failure is a failure message.

The reminder ring option (which is available with the DND feature on MGCP-based lines) cannot be used with SIP devices.

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

Caution Prior to provisioning your system, determine how you want to apply and configure features in your network to avoid conflicts between features provided by the BTS 10200 and features provided by the phones.

Additional information on this feature is provided at the following links.

Provisioning Procedure	Feature Behavior (Feature Description and Handset Provisioning)
"Do Not Disturb (DND)" section in the *Cisco BTS 10200 Softswitch Provisioning Guide*	"Do Not Disturb (DND)" section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document

E.164 and Centrex Dialing Plan (Extension Dialing)

The system supports E.164 and Centrex Dialing Plan (extension dialing) addressing from SIP subscribers served by the local BTS 10200.

The SIP phone's dial plan must be configured so that it considers the number of digits in the Centrex group. Centrex dialing can be provisioned within a range of 1 through 7 digits. Each Centrex group should have its own separate dial plan.

Note   The CDP feature should be assigned to every Centrex category user.

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

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

Additional information on this feature is provided at the following links.

Provisioning Procedure	Feature Behavior (Feature Description and Handset Provisioning)
"Provisioning a Centrex Group" section in the *Cisco BTS 10200 Softswitch Provisioning Guide* *Cisco BTS 10200 Softswitch Dial Plan document*	"Numbering Plans and Dialing Procedures" section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document "Features for Centrex Subscribers Only" section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document

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

There is no Cisco BTS 10200 Softswitch subscriber-specific provisioning involved for Operator Services.

Additional information on this feature is provided in the "Operator Services" section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document

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.

Vertical Service Code Features

This section explains how to plan vertical service codes (VSCs) in a network with SIP subscribers, and lists the VSC-enabled features.

Planning VSCs In Networks with SIP Subscribers.

Some features require SIP subscriber to enter a series of numbers and characters on the SIP client or handset. Typically, the subscriber dials VSC digits followed by additional dialing keys representing the parameters for the feature call. For MGCP subscribers, the BTS 10200 sends a response tone or announcement between the VSC code and the additional digits. However, for SIP endpoints, all the digits are dialed at a stretch without waiting for an intervening response tone from the BTS 10200. The following paragraph explains how certain combinations of VSC can cause mismatches between the feature the subscriber is attempting to manage versus the response of the BTS 10200, and how to plan VSCs to avoid these mismatches.

You should not deploy certain combinations of VSCs on networks with SIP endpoints. If you deploy a VSC longer than 2 digits, make sure that the longer VSC does not begin with the same sequence of characters as one of the shorter VSCs. In some cases, the system might match the shorter string even if the subscriber dialed the longer string. Consider the following example, for which the subscriber is expected to dial a VSC followed by a DN.

A SIP subscriber is provisioned with *93 for Feature1 and *938 for Feature2, and dials *938+2135551801 to invoke Feature2. The BTS 10200 receives *9382135551801 in the INVITE message. By default, it takes the first six characters, in this case *93821, and uses this string to look up the feature in the VSC table. There is no match for *93821, therefore the BTS 10200 proceeds as follows. First, it uses *9 to look for a match in the VSC table and it cannot be found. Then it uses *93, finds a match, and delivers Feature1. This is incorrect. The user's intention was to invoke Feature2 and not Feature1. The solution is for the service provider to change one of the two VSCs (either *93 or *938) in the VSC table.

Supported VSC-Enabled Features for SIP Endpoints

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

- Calling identity delivery and suppression, suppression part (CIDSS)
- Calling identity delivery and suppression, 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)

Reminder ringback cannot be enabled for SIP subscribers. If you are 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.

Here is the command format at the feature level:

```
add feature fname=CFU; tdp1=TERMINATION_ATTEMPT_AUTHORIZED;
tid1=TERMINATION_ATTEMPT_AUTHORIZED; feature_server_id=FSPTC235; ttype1=R;
fname1=CFUA; fname2=CFUD; type1=MCF; value1=Y; type2=RR; value2=N;
description=CFU MCF multiple call forwarding allowed, RR ring reminder not
allowed;
```

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

Voice Mail

The voice-mail (VM) feature on the BTS 10200 allows subscribers to retrieve waiting voice messages from a VM server. The BTS 10200 receives a message-waiting indication (MWI) from the VM server and forwards the MWI to the subscriber's handset. The subscriber can then retrieve messages from the server. The VM feature is available to individual subscribers and Centrex subscribers.

SIP trunks interconnecting the BTS 10200 to an external VM server must be provisioned as SIP VM trunks. To do that, you set the VM flag (voice-mail-trunk-grp) for these trunks in the softsw-tg-profile table. (See the "SIP Trunk to Voice-Mail Server" section on page 3-46.)

Note   For a description of the basic VM feature, see the "Voice Mail and Voice Mail Always" section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document. For general VM provisioning details, see the "Provisioning Voice Mail" section in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

VM Actions

The following voice mail-related actions are supported in the BTS 10200:

- VM Deposit
- MWI Notification
- Retrieving VM
- Calling Back a Message Depositor

VM Deposit

There are two methods for depositing voice mail. In the first, the subscriber dials the pilot number for the VM server, and the call terminates on the voice-mail trunk. The VM system then collects the message for a target mailbox, using Interactive Voice Response (IVR) prompts to guide the subscriber.

This method of depositing voice mail does not use any special BTS 10200 capabilities; it just requires that the VM SIP trunk is provisioned and the pilot number is added to the dial plan of the subscriber calling the VM system.

In the second (more common) method, the subscriber activates a call forwarding feature on the BTS 10200, such as CFNA, CFU, or CFB, and specifies the forwarding number as the pilot number of the VM server.

MWI Notification

When a SIP phone registers with the BTS 10200, the BTS 10200 sends an unsolicited SIP NOTIFY message to convey the MWI status to the phone. This occurs on every registration, including refreshes.

Whenever a change in VM status occurs for a subscriber (for example, when a VM message is deposited for the subscriber, or when all such messages have been retrieved), the VM server sends an update to the BTS 10200. If the subscriber is on a SIP phone, the BTS 10200 sends an unsolicited SIP Notify message to convey the MWI status to the phone. The number in the Notify message Request URL (which is the assigned subscriber number) identifies the subscriber.

When the BTS 10200 is congested by a flood of registrations (which might occur, for example, when power is restored to a region after an outage), it can automatically suppress the MWI indication to the registering phones, so that registration throughput is not adversely affected.

The BTS 10200 implements the draft-ietf-sipping-MWI-01.txt with the following caveat: It supports receiving unsolicited NOTIFYs from a VM system; however, it does not support subscribing to these notifications. Further, the BTS 10200 does not support subscriptions for MWI. It sends unsolicited NOTIFYs for MWI to SIP subscribers. No subscription is expected from the SIP phones for the purpose of receiving this notification.

The notification of MWI by the BTS 10200 is enabled by default (VMWI=Y in the Subscriber table). You can disable it by setting VMWI=N.

Tip   For MGCP subscribers, the BTS 10200 sends the MGCP RQNT message to turn on MWI on the analog phone. This activates the MWI indicator on the subscriber phone. The indicator can be visual (a lamp, an envelope, or another icon on a display) or it can be auditory, such as a stutter dial tone that is provided when the user next goes off-hook.

For information on setting the MWI and VMWI parameters in the Subscriber table, see the "Message Waiting Indicator (MWI)—Audible and Visual" section in the *Cisco BTS 10200 Softswitch Network and Feature Descriptions* document.

Retrieving VM

To retrieve a VM message, subscribers dial the pilot number for the VM server. The BTS 10200 routes the call to the SIP trunk for VM, based on the provisioned dial plan for the subscriber and the route, destination, and trunk-group entries.

Once the VM message is retrieved, the VM server sends a Notify message to the BTS 10200 to turn off the MWI indicator.

Calling Back a Message Depositor

When subscribers call into a VM server, this feature allows for calling back the person who left the voice-mail message. The feature requires that a Softswitch trunk for the VM server be provisioned in the Cisco BTS 10200 Softswitch with the relevant routes, destination, and dial plans in order to admit VM-originated calls into the BTS 10200.

VM Implementation for Centrex Subscribers

For calls received on SIP VM trunks from the VM server, a subscriber is provisioned and associated as the main sub-ID for each trunk. The subscriber information represents properties of a specific Centrex group and does not represent any particular subscriber. No AOR is provisioned for this subscriber. This information is used for call processing.

> ✎
> **Note**   For general VM provisioning details, see "Provisioning Voice Mail" in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

VM Within a Single Centrex Group

The following examples show commands for provisioning Centrex VM. Before you perform the following steps, you must already have a Centrex group provisioned on your system. See the procedure in the "Provisioning a Centrex Group" section of the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Step 1   Add the destination ID for the voice-mail main subscriber.

```
add destination dest-id=tb16-local; call-type=LOCAL; route-type=SUB;
```

Step 2   Add a dial plan profile and dial plan for a SIP trunk to the VM server.

```
add dial-plan-profile id=tb16;

add dial-plan id=tb16; digit-string=469-555; dest-id=tb16-local; min-digits=10;
max-digits=10
```

Step 3   Add the softswitch trunk group profile for voice mail.

```
add softsw-tg-profile id=VM_Profile; protocol-type=SIP; voice_mail_trunk_grp=Y;
```

> ✎
> **Note**   As an option, you can provision the diversion-header-supp token in the softsw-tg-profile table to Y. This instructs the VM server to select the target inbox based on the original called number in the Diversion header of the SIP message.

Step 4   Add the SIP trunk group.

> ✎
> **Note**   This SIP trunk group serves several purposes. It is used (1) by the subscriber to access the VM server, (2) by the BTS 10200 to forward incoming calls to the VM server, and (3) by the VM server to notify the BTS 10200 that a message is waiting for the subscriber.

```
add trunk-grp id=80032; softsw-tsap-addr=vm.domainname.com:5060;
call-agent-id=CA146; tg-type=softsw; tg-profile-id=VM_Profile; dial-plan-id=tb16
```

Step 5   Add a subscriber to the Centrex group to serve as the VM main subscriber.

```
add subscriber id=vmctxg1; CATEGORY=ctxg; BILLING-DN=469-555-4444;
DN1=469-555-4444; SUB-PROFILE-ID=Centrex_sp2; TERM-TYPE=TG; ctxg_id=ctxgsip1;
tgn_id=80032;
```

Step 6   Link the VM main subscriber with the trunk group.

```
change trunk-grp; id=80032; main_sub_id=vmctxg1;
```

Step 7   Map the voice-mail Centrex extension to the VM main subscriber.

```
add ext2subscriber CTXG-ID=ctxgsip1; EXT=54444; CAT-CODE=1; SUB-ID=vmctxg1;
```

Step 8   If your VM server does not support FQDN hostnames, you must provision a serving-domain-name record in the BTS 10200 using the IP addresses resolved from the sia-xxxCAnnn.domain address. Otherwise, the VMWI status from SIP voice-mail platforms fails authentication with the BTS 10200. The details for this step are provided in Step 6 of the "SIP Trunk to Voice-Mail Server" section on page 3-46,

Provisioning Voice Mail Across Multiple Centrex Groups

A VM application server can provide VM service for Centrex subscribers from multiple Centrex groups on the BTS 10200. For the VM server to identify the subscriber and provide service configured for a Centrex group, the BTS 10200 must indicate the Centrex group with which the subscriber is associated,

When the BTS 10200 forwards a call from a Centrex extension to VM, the VM server identifies the Centrex group of the extension to deposit the message in the correct mailbox. Further, when the VM server sends a SIP Notify message to indicate that messages are waiting for a Centrex subscriber on the BTS 10200, it must identify the Centrex group in the request URI of the NOTIFY message sent to the BTS 10200.

For any INVITE sent out a SIP trunk by the BTS 10200 to the VM server, a BTS 10200 proprietary SIP URL parameter **bgid** is added to the From, To, Diversion, and Request URIs, if the user part of those URLs contains a Centrex extension number format in the user information field. The **bgid** value is provisioned as the trunk-subgroup-type on the SIP trunk, and identifies the Centrex group.

An example of this parameter syntax follows:

```
INVITE sip:50001@vm.cisco.com:5060;user=phone;bgid=grpA SIP/2.0
From: <sip:50603@bts.cisco.com;user=phone;bgid=grpA>;tag=1_1146_f40077_3jwv
To: <sip:50586@bts.cisco.com;user=phone;bgid=grpA>
Diversion: <sip:50586@bts.cisco.com;bgid=grpA>;reason=unconditional;counter=1
```

When the VM server notifies the BTS 10200 of a MWI for a Centrex subscriber, the VM server sends a Notify SIP request to the BTS 10200 with a Centrex number format in the Request URL, and an associated bgid parameter identifying the Centrex group associated with the subscriber. When the VM server initiates a call to a BTS 10200 Centrex subscriber for VM callback functionality, bgid is added to the request URL of the initial INVITE originating from the VM server. This identifies the Centrex group associated with the subscriber.

The BGID parameter in the ReqUri of an INVITE originated from the VM server identifies the called subscriber in the targeted Centrex group. For example, the BGID parameter in the ReqUri of a NOTIFY message from the VM server to the BTS 10200 identifies the subscriber in the targeted Centrex group whose MWI lamp is turned on or off.

The BTS 10200 does not support extension-dialed calls from one Centrex group to another. Therefore, the **bgid** parameter has an identical value if it is present in any of the URLs in the From, To, Diversion, and Request URL headers for a given INVITE message. The trunk group configuration includes a trunk subgroup field for specifying the **bgid** parameter value. One trunk group is provisioned for each Centrex group; the **bgid** parameter in the trunk group table is unique to the specific Centrex group. Routing tables are configured so that each trunk handles SIP calls to and from the VM server for a specific Centrex group. To qualify a specific trunk for **bgid** and VM, provision as follows:

- In the Trunk Group (trunk-grp) table, provision the **bgid** value in the trunk-sub-grp field.
- In the Softswitch Trunk Group Profile (softsw-tg-profile) table:
  - Provision the trunk-sub-grp-type field as BGID.
  - Provision the voice-mail-trunk-grp field as Y.

The following provisioning steps illustrate how to provide VM service for BTS 10200 Centrex subscribers across multiple Centrex groups.

Step 1   Add a SIP trunk profile for voice-mail trunks. Qualify voice-mail trunks by setting the voice-mail flag, and set the trunk sub-group type to indicate use of business group identifier:

```
add softsw_tg_profile ID=<profile_id>; PROTOCOL_TYPE=SIP;
VOICE_MAIL_TRUNK_GRP=Y; TRUNK_SUB_GRP_TYPE=BGID;
```

Step 2   Add a SIP trunk for each business group identifier. Each trunk points to the address of the voice-mail sever.

In the following command, be sure to enter a unique business group identifier for each Centrex group, for example, **bg1**, **bg2**, and **bg3**, for the three Centrex groups in this example.

Also, be sure to specify the FQDN and port that the VM server uses for SIP message exchange, for example, **vmserver:5060**.

```
add trunk_grp ID=<trk_grp_id1>; TG_TYPE=SOFTSW; TG_PROFILE_ID=<profile_id>;
SOFTSW_TSAP_ADDR=vmserver:5060; DIAL_PLAN_ID=dp; TRUNK_SUB_GRP=bg1;

add trunk_grp ID=<trk_grp_id2>; TG_TYPE=SOFTSW; TG_PROFILE_ID=<profile_id>;
SOFTSW_TSAP_ADDR=vmserver:5060; DIAL_PLAN_ID=dp; TRUNK_SUB_GRP=bg2;

add trunk_grp ID=<trk_grp_id3>; TG_TYPE=SOFTSW; TG_PROFILE_ID=<profile_id>;
SOFTSW_TSAP_ADDR=vmserver:5060; DIAL_PLAN_ID=dp; TRUNK_SUB_GRP=bg3;
```

Step 3   Create a dial plan for calls received on the SIP trunks, so that they can be routed based on the called party number. For example, the identifier for the dial plan in this example is **dp**. (The dial plan provisioning details are not shown here.) The Centrex group routing and dial plan tables should be provisioned so that calls originating from a specific Centrex group subscriber are sent out the SIP trunk with the business group identifier representing that Centrex group.

Jointly Provided Features

Some features are provided jointly by the phone and by the BTS 10200. Here are some examples:

- Text-GUI Features
- Call Transfer (Blind and Attended) with REFER
- Distinctive Ringing
- Distinctive Ringing for Centrex DID Calls

The sections that follow provide information about these features.

Text-GUI Features

The BTS 10200 supports SIP client/handset text-based user interface (UI) provisioning for a select set of features. This is in addition 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 complementary 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 might be multiple lines on the SIP phone, but currently services configured by softkeys on the phone are available to only one of those lines. The subscriber for that line is provisioned in the BTS 10200 with the MAC address of the phone (see the MAC Address to Subscriber table in the Cisco BTS 10200 Softswitch CLI Database).

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 indicating "Services." Initial access to feature provisioning is through the Services button. After initial access, the UI display area provides a menu-driven interface and a feature-specific menu.

To navigate the menu, the end user presses the Up and Down arrow buttons or menu numbers. At any level of navigation, the end user presses the Exit softkey to go back one step in the menu hierarchy. The user selects menu items using the Select softkey button and uses the numeric dial 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 user interface.

Call Transfer (Blind and Attended) with REFER

The SIP Call Transfer (CT) feature is supported for SIP subscribers. For SIP phones, this feature is provided as part of REFER support on the BTS 10200.

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

The difference between provisioning the feature for SIP and provisioning it for MGCP is as follows:

- Call transfer on both the Cisco IP Phone 7905/7912 and the Cisco IP Phone 7940/7960 is done using softkeys. On the Cisco ATA 186/188, call transfer is done using the Flash key (or by pressing the on-hook button briefly) on the analog phone attached to the Cisco ATA 186/188.

- Call-transfer functionality for SIP-based systems is performed using the REFER feature, *not the traditional call transfer (CT) feature*. To enable CT for SIP subscribers, you must provision the REFER feature as an office trigger in the Cisco BTS 10200 Softswitch. See the for additional details and provisioning procedures.

Distinctive Ringing

Distinctive ringing uses a special ringing pattern to alert the called user of incoming calls from preselected telephone numbers. This is a CLASS feature and is offered to both business and residential users. There is no difference between provisioning the feature for SIP and provisioning it for MGCP.

You can edit the list of selected numbers though the Screening List Editing (SLE) feature, which requires the configuring of an IVR with the BTS 10200. Distinctive ringing can be assigned to a station and to the group, and it can be 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 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 an Alert-Info header.

Distinctive Ringing for Centrex DID Calls

The 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 process the information received in the Alert-Info header. There are no differences between provisioning the feature for SIP and provisioning it for MGCP.

Phone-Based Features

The phone provides some features standalone, without BTS 10200 support. If the SIP phone requires provisioning to provide this function, refer to the SIP phone documentation for instructions.

Table 2-3 lists the phone-based features.

.

Table 2-3   ***SIP Phone-Based Features***

Feature	Acronym
Call Hold and Resume	CHD
Call Waiting	CW
Call Waiting Caller ID	CWCID
Cancel Call Waiting	CCW
CODEC Up-Speeding	CODEC[1]
Do Not Disturb	DND
Three-Way Calling	TWC

1. For feature calls between MGCP and SIP subscribers, the BTS 10200 supports the CODEC up-speeding capability. The SIP phone would also need to support this capability for the up-speeding capability to be fully supported in the call.

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

⚠

Caution   Prior to provisioning your system, determine how you want to apply and configure features in your network to avoid conflicts between features provided by the BTS 10200 and features provided by the phones.