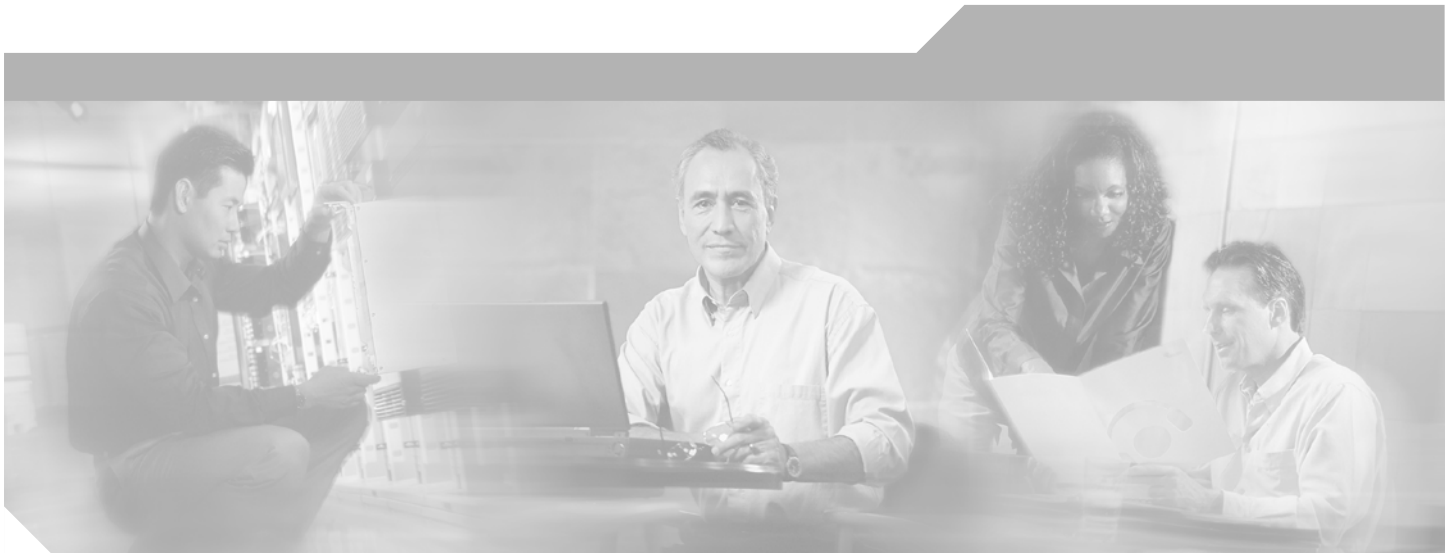


Cisco BTS 10200 Softswitch SIP Protocol User Guide Release 4.5.x

Revised May 3, 2007

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

Customer Order Number:
Text Part Number: OL-5352-12

Cisco BTS 10200 Softswitch SIP Protocol User Guide Release 4.5.x

Preface

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

The *Cisco BTS 10200 Softswitch SIP Protocol User Guide* details support for Session Initiation Protocol (SIP) devices and trunks in Release 4.5.x. This guide covers areas impacted by the feature and is an addition to the existing Cisco BTS 10200 Softswitch documentation.

Revision History for Release 4.5.x

This document includes all of the information that was contained in the previous issues (the Release 4.4 SIP Protocol User Guide), and has been updated as follows for Release 4.5.x.

Cisco BTS 10200 Softswitch Release	Changes
Release 4.5.x, continued	OL-5352-12: (Release 4.5.1, Maintenance Release 2) Information was added regarding the contents of the Diversion headers and presentation values. See the "Diversion Indication" section on page 2-31 and "Diversion Indication" section on page 3-11. OL-5352-11: (Release 4.5.1, Maintenance Release 2) Information was added regarding the number of parameters in headers. See the "Limitations on Number of URLs, Parameters, and Headers (Release 4.5.1, Maintenance Release 2)" section on page 1-17. OL-5352-10: Clarification was added that provisioning changes to DSCP parameters in the ca-config table do not take effect until the CA platform restarts or switches over (Chapter 2, "SIP Protocol Subscriber Features" and Chapter 3, "SIP Protocol Trunk Features"). OL-5352-09: • Added a note regarding changed SDPs in the "SIP Timer Values" section on page 2-23 and the "Session Timers" section on page 3-14. • Corrected the information on SIP support for the Calling Number Delivery (CND) feature in Appendix A "MGCP Features vs. SIP Features."

Cisco BTS 10200 Softswitch Release	Changes
Release 4.5.x, continued	OL-5352-08: • (Release 4.5.0 and 4.5.1) Added information about treatment of transient calls in Chapter 1, "SIP Devices Support Overview." • (Release 4.5.0 and 4.5.1) Added information about user-level privacy in Chapter 2, "SIP Protocol Subscriber Features." • (Release 4.5.0 and 4.5.1) Added information about 3XX call redirection in Chapter 3, "SIP Protocol Trunk Features." • (Release 4.5.1, Maintenance Release 1) Added a section about source IP validation in Chapter 3, "SIP Protocol Trunk Features." • (Release 4.5.0 and 4.5.1) Added the value of USER for the privacy parameter in the Subscriber table in Chapter 5, "Database Tables."
Release 4.5.x	OL-5352-07—The following information was changed: • SIP Timer Values, page 2-23: Added drawings to illustrate the usage of several SIP timers. • TRUNK-GRP Table, page 3-22: Removed unused tokens. The following features were added or enhanced in Release 4.5.x: • Phone-Based Features, page 1-15 • SIP Devices, page 2-2 • Enhanced SIP Registration, page 2-4 • Session Timers, page 2-22, and SIP Timer Values, page 2-23 • T.38 Fax Relay Call Agent Controlled Mode Across SIP Trunk Interface, page 3-24 • SIP Dynamic Memory Audit, page 2-18 • Outbound Cisco BTS 10200 SIP Call, page 3-2 • SIP Trunk Features, page 3-2 • Chapter 4, "Voice-Mail Support" • Chapter 5, "Database Tables" For additional new or modified SIP features, refer to New or Enhanced SIP Subscriber Features for Release 4.5.x, page 1-8.

Audience

This guide is intended for use by service provider management and system administration personnel who are responsible for installing, provisioning, and maintaining networks that use the Cisco BTS 10200 Softswitch system.

Organization

This document is organized as follows:

- Chapter 1, "SIP Devices Support Overview"
- Chapter 2, "SIP Protocol Subscriber Features"
- Chapter 3, "SIP Protocol Trunk Features"
- Chapter 4, "Voice-Mail Support"
- Chapter 5, "Database Tables"
- Chapter 6, "Measurements, Events, and Alarms"
- Appendix A, "MGCP Features vs. SIP Features"

Conventions

This document includes the following conventions:

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

Related Documents

Use this document in conjunction with the following Cisco BTS 10200 Softswitch documents:

- *Cisco BTS 10200 Softswitch Release Notes for Release 4.5.x*
- *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*
- *Cisco BTS 10200 Softswitch Physical and Network Site Surveys and Data Sheets*
- *Cisco BTS 10200 Softswitch Cabling Procedures*
- *Cisco BTS 10200 Softswitch System Description*
- *Cisco BTS 10200 Softswitch Application Installation Procedures*
- *Cisco BTS 10200 Softswitch Operations Manual*
- *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions*
- *Cisco BTS 10200 Softswitch Billing Interface Guide*
- *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*
- *Cisco BTS 10200 Softswitch CORBA Installation and Programmer's Guides*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

SIP Devices Support Overview

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

The purpose of this guide is to detail the Session Initiation Protocol (SIP) device support, and the changed trunk support in Release 4.5.x. Support for SIP trunks existed in previous releases of the Cisco BTS 10200 Softswitch, but support for SIP devices was new in Release 4.1. The user guide covers areas impacted by the SIP feature, and is an addition to the existing Cisco BTS 10200 Softswitch documentation.

Note The term "SIP devices" refers to Cisco ATA 186/188 adaptors, and to Cisco IP phones.

The SIP support feature provided in Release 4.5.x was built on the existing Cisco BTS 10200 Softswitch software and hardware platform. The user guide describes the features and protocol changes in Cisco BTS 10200 Release 4.5.x for supporting SIP trunks and subscribers.

The Cisco BTS 10200 Softswitch complex includes a Call Agent (CA), Feature Server (FS), Element Management System (EMS), and an optional HTTP feature server (HTTP-FS) which is comprised of a GUI Feature Server (GUI-FS) and Mini-Browser Adapter (MBA). In this book, all references to the term "Cisco BTS 10200" refer to the Call Agent unless otherwise specified.

SIP protocol support for subscriber features is provided by the Call Agent and the POTS Feature Server.

The Cisco BTS 10200 Softswitch uses SIP and SIP for telephones (SIP-T) signaling to communicate with other SIP-based network elements. The implementation is based upon the evolving industry standards for SIP, including IETF document RFC 3261, SIP: Session Initiation Protocol. The Cisco BTS 10200 Softswitch supports both SIP trunks and SIP-based subscriber lines (SIP devices), and provides the following SIP-related functions:

- Protocol conversion between SIP and several other protocols, including SS7, PRI, ISDN, H.323, MGCP, and CAS.
- Tandem back-to-back user agent for direct SIP-to-SIP calls (trunk to trunk, phone to phone, and trunk to/from phone), and SIP-to-SIP-T calls.
- SS7 bridging between Softswitches using SIP-T methods.
- Native support of SIP endpoints such as SIP phones, including authentication and registration management. (For example, the Cisco BTS 10200 Softswitch maintains the current location of SIP subscribers.)

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

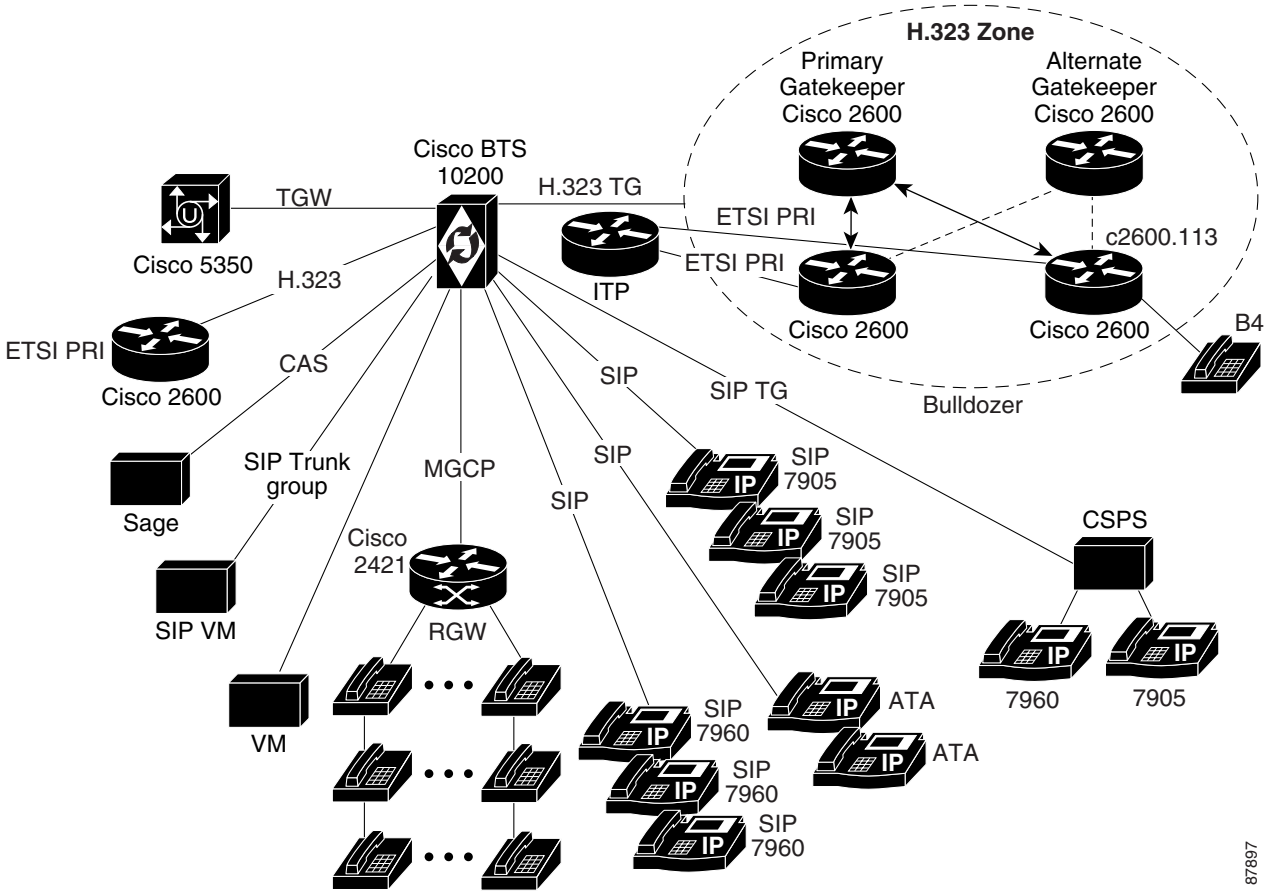
SIP Roles Played by Cisco BTS 10200 Softswitch

Figure 1-1 shows the new Cisco BTS 10200 Softswitch architecture with native support for SIP phone subscribers. In addition to its existing capabilities, in this new architecture, Cisco BTS 10200 provides Registrar (with SIP user authentication) services.

The Cisco BTS 10200 Softswitch supports call processing for SIP trunks and phone users. As a result of native SIP subscriber support, SIP subscribers can use features formerly available only to MGCP subscribers.

For a comparison of the MGCP and SIP feature support, see Appendix A, "MGCP Features vs. SIP Features."

Figure 1-1 Cisco BTS 10200 Softswitch Network Architecture



SIP roles performed by the Cisco BTS 10200 Softswitch include:

- User agent server (UAS)
- User agent client (UAC)
- Registrar

Note The Cisco BTS 10200, as part of the Back-to-Back functionality, plays the role of the UAS and UAC.

Most features provided by the SIP phones comply with LATA Switching Systems Generic Requirements (LSSGR), depending on the phone implementation and capabilities. Due to the nature of the SIP protocol, however, your experience with a feature may differ from what is documented in the LSSGR for that feature.

Limitation On Treatment of Transient Calls

If the active Call Agent experiences a problem and switches over to the standby side, stable calls are preserved. However, calls that are in a transient state (call setup is not complete) might be dropped or improperly set up. During a Call Agent switchover, the Cisco BTS 10200 Softswitch cannot complete call setup for these transient calls.

Transient calls and inactive connected calls originated on the Cisco BTS 10200 Softswitch are cleaned up through a periodic audit mechanism that runs once per hour. The frequency of this audit can be modified. However, changing this requires careful consideration to avoid adverse effects on call processing. Contact Cisco TAC if you have identified a need to change this frequency.

SIP Phone Registrar

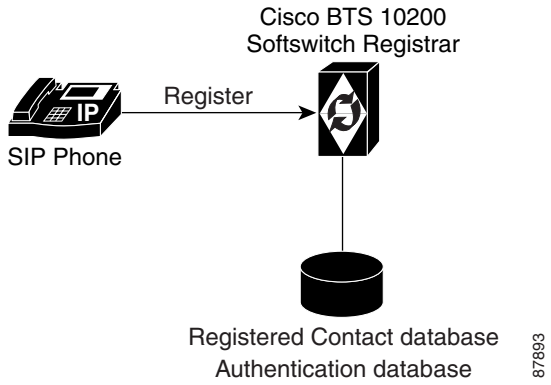
SIP Register support enables SIP devices to be served by Cisco BTS 10200 directly without a proxy. The Cisco BTS 10200 acts as a Registrar and authenticates the SIP request.

To initiate a session with a SIP phone, Cisco BTS 10200 must know the current address of the phone. Registration creates bindings in a location service for a particular domain that associate an address-of-record Uniform Resource Identifier (URI) with one or more contact addresses. A user notifies its availability at the address provided in the contact for the specified duration.

The SIP phone registers with Cisco BTS 10200, setting up a binding between the Address of Record (AOR) and its contact address. The registration is valid for a period of time until it expires.

Figure 1-2 demonstrates the SIP phone Registrar function.

Figure 1-2 SIP Phone Registrar Function



Cisco BTS 10200 supported SIP subscribers with SIP phones starting in Release 4.1. SIP users register with Cisco BTS 10200 and originate calls through Cisco BTS 10200. To identify the SIP user, Cisco BTS 10200 uses the challenge-based Digest Access Authentication.

User Agent Client and User Agent Server

The User Agent is a SIP endpoint (such as a phone or a gateway). In this scenario, the User Agent is software running on the endpoint to enable SIP service.

The User Agent can work either as a client or server. When a call is placed, the User Agent Client (UAC) places the request, and the User Agent Server (UAS) services the request and sends a suitable response. The roles change continually, however; for example, with call hold, either user can put the other user on hold.

Figure 1-3 shows the Cisco BTS 10200 working as a UAC, sending out a call request.

Figure 1-3 User Agent Client

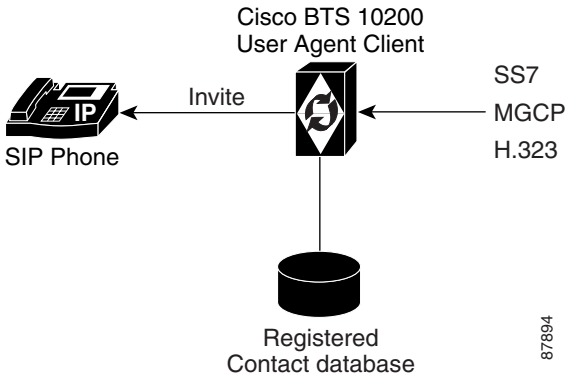
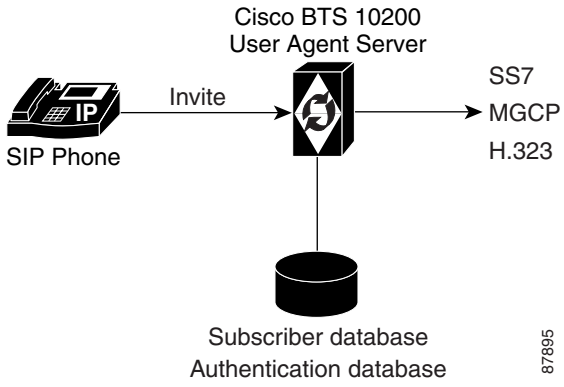


Figure 1-4 shows the Cisco BTS 10200 working as a UAS, accepting a call request.

Figure 1-4 User Agent Server



Back-to-Back User Agent

The back-to-back user agent acts as a UAC and UAS for a single call. It keeps the two call segments separate on the Cisco BTS 10200 Softswitch. Typically, a proxy routes a call, but does not act as a User Agent. The Cisco BTS 10200 acts as a User Agent. In a call between two SIP endpoints (such as SIP phone or SIP trunk), Cisco BTS 10200 terminates the originating half of the call, playing the UAS role, and then sets up the terminating half of the call as a UAC.

Note There is no provisioning associated with the back-to-back functionality. The Cisco BTS 10200 automatically acts as a back-to-back user agent for a SIP to SIP call.

Figure 1-5 shows the Cisco BTS 10200 working as a back-to-back user agent.

Figure 1-5 Back-to-Back User Agent Server

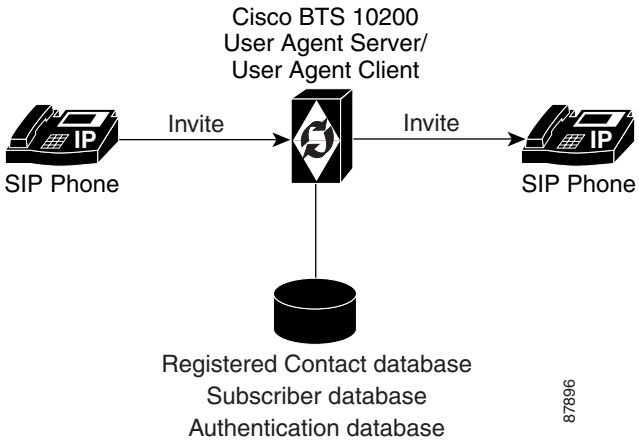


Figure 1-5 shows the call flow for registration.

Figure 1-6 Call Flow for Registration

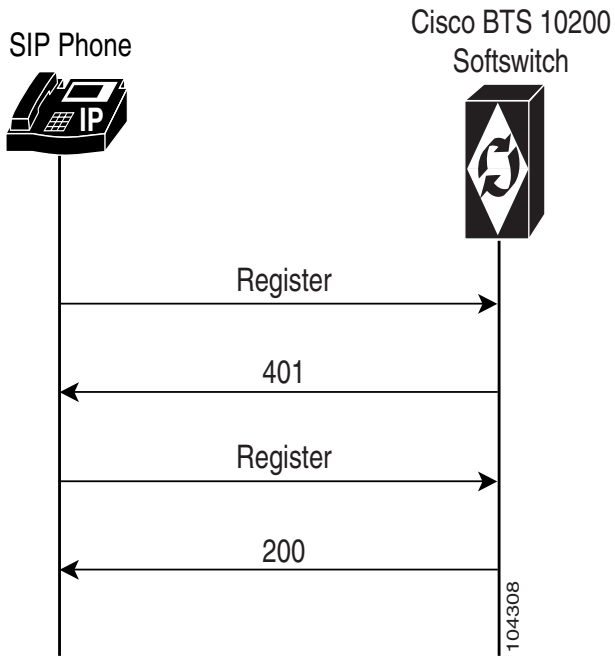
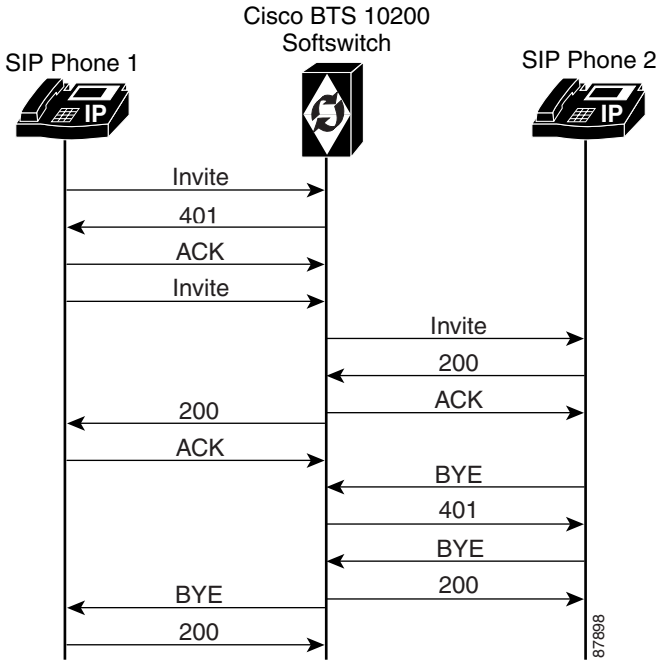


Figure 1-7 shows the call flow for a back-to-back User Agent.

Figure 1-7 Back-to-Back User Agent Call Flow with Authentication



SIP Subscriber Features

SIP Subscriber features are categorized as follows:

- Cisco BTS 10200 Softswitch-Based Features—These are provided entirely by the Cisco BTS 10200, and require suitable provisioning of the Cisco BTS 10200.
- Phone-Based Features—These are provided exclusively by the phone, which require provisioning on the phone.
- Jointly-Provided Features—These are provided jointly. The features are provided partly by the phone's capability, and partly by Cisco BTS 10200 capabilities. To use these features, you must provision both the phone and the Cisco BTS 10200.

New or Enhanced SIP Subscriber Features for Release 4.5.x

Table 1-1 lists the new or enhanced SIP features supported in Release 4.5.x.

Table 1-1 New Cisco BTS 10200 Softswitch-Based SIP Features

SIP Feature	Description	For More Information
T.38 Fax Relay Call Agent Controlled Mode Across SIP Trunk Interface	In previous releases, Cisco BTS 10200 partially supported T.38 fax relay call agent controlled mode in MGCP and H.323 trunk interfaces. Release 4.5.x offers supports for the PacketCable environment, as well as extending T.38 fax support to SIP, NCS, and TGCP trunk interfaces.	Refer to the *T.38 Fax Relay* feature module.
Secure Provisioning for SIP Endpoints	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. The feature also ensures that the source IP address and contact parameter for all originating calls is from the provisioned SIP endpoint, and that no calls can originate from an unregistered endpoint.	Refer to the *Secure Provisioning for SIP Endpoints* feature module.
SIP Session Timers	SIP Session Timer values configured prior to Release 4.5.x are reset to the default values after upgrading to Release 4.5.x.	Refer to SIP Timer Values, page 2-23 for an overview description. For provisioning information, refer to Session Timers in the *Cisco BTS 10200 SIP Provisioning Guide*.
SIP Dynamic Memory Audit	Refer to SIP Dynamic Memory Audit, page 2-18 for a more in-depth description.	Also, refer to the Activity table section in the *Cisco BTS 10200 Command Line Interface Reference Guide*.

Table 1-1 New Cisco BTS 10200 Softswitch-Based SIP Features

SIP Feature	Description	For More Information
SIP Transport	When a 503 response is received, the entity receiving the response proceeds by submitting the same request as a new transaction (with new branch ID) to the next IP address in the SRV list. Previously, when SIA received the 503 response, it tore down the call. As a result, some calls may not have completed if one of the nodes in an SRV list returned the 503, while other nodes in the list were capable of handling the request successfully. If an SRV server receiving the INVITE does not respond within the retransmission timer period, this enhancement allows for configuring the Cisco BTS 10200 to send the next retransmission of the same request to either the same server (as recommended in RFC3263) or the next server in the SRV list (legacy Cisco BTS 10200 behavior) using a provisionable flag DNS_SRV_ADV_ON_RETRANS_TIMEOUT on the SOFTSW-TG-PROFILE table.	
INVITE Retries Are Configurable	The SIP protocol adapter enables the configuration of the number of INVITE and non-INVITE retries on timer expiry (instead of the fixed 6), and also makes the retry timers configurable. This improves route advancing and completes calls more quickly if one IP address is down. SIP timers are configurable on a per trunk basis, or on a system wide basis for all non-trunk messages. The number of retries and retry interval could be tuned using RFC3261 timers. The guidelines and recommendations on configuring SIP timers will be available in the *Cisco BTS 10200 SIP Protocol User Guide*. The timers are configurable on a global basis through the Softswitch Trunk Group Profile (SOFTSW Trunk Group Profile) and Call Agent Configuration (CA-CONFIG) tables.	Refer to the SOFTSW Trunk Group Profile and CA-CONFIG sections in the *Cisco BTS 10200 Command Line Interface Reference Guide*.
SIP Retry	SIP responses received from a Re-Invite or Update sent during an active call that contain a Retry-After header invoke the SIA retry mechanism. Currently, this includes only the SIP 500 class response. The check has been expanded to include other responses.	
SIP Stack Message Size	Previous to Release 4.5.x, the SIP stack could only send and receive messages up to 1500 bytes in size from the network. If a message was bigger than 1500 bytes, only the first 1500 bytes were read and parsed. Release 4.5.x fixes the limitation imposed on the maximum size of the SIP messages which can be sent or received. The SIP stack can now receive/send SIP messages up to 3000 bytes in size.	

Table 1-1 New Cisco BTS 10200 Softswitch-Based SIP Features

SIP Feature	Description	For More Information
SIP Trunk Hop Counter	The SIP Trunk Hop Counter feature was added into Cisco BTS 10200 Release 4.1, but was not provisionable. However, the feature's provisionable components are available in Release 4.5.x, and are provisionable using the SOFTSW Trunk Group Profile table: • HOP-COUNTER-MAX • HOP-COUNTER-SUPP • MAX-FORWARDS **Note** Seven SIP hops are equivalent to one SS7 hop.	For more information, refer to the SOFTSW Trunk Group Profile section in the *Cisco BTS 10200 Command Line Interface Reference Guide*.
Cisco BTS 10200 Sends SDP for SIP Call When rbk=N for Call Waiting	When a SIP call inbound to the Cisco BTS 10200 is routed to a local subscriber, and this call causes "call waiting" at the subscriber, the originator is provided local ringback indication. However, in this case, the SIP interface was providing remote ringback indication. This may result in the originator not hearing ringback or possibly the discussion of the other dialog. The SIP interface was corrected to provide local ringback.	
SIA Diversion Header	Previously, when one diversion header was received in the initial SIP Invite message, the Original Called Number (OCN) was populated. To be consistent with other adapters, the value is now copied to the Redirect Number (RDN) as well.	
SIP Outbound Numbers Require +CC Depending on NOA	RFC 3398 states that any outbound SIP number with NOA of NATIONAL must be prefixed with "+CCnumber" which is an international format, and any number with NOA=subscriber must be formatted also with international significance. This was not done in previous releases. Sending Full E.164 is enabled by a flag in softsw-tg-profile to enable interworking with downstream devices that require this number format.	
SIP Stack	SIP message loop detection was removed in Release 4.5.x. Previously, the SIP stack did not allow receipt of an un-changed Request URI on hairpinned INVITEs. This required the entity that was hairpinning the SIP call back to Cisco BTS 10200 to modify the user portion of the Request-URI, so that Cisco BTS 10200 does not detect a loop. Since adding the Digman feature, the digit manipulation is performed within Cisco BTS 10200, thereby preventing a requirement for this check. As such, this check is a configurable option that can be toggled through SIA's configuration file for SIP stack.	

Table 1-1 New Cisco BTS 10200 Softswitch-Based SIP Features

SIP Feature	Description	For More Information
DOMAIN-NAME Verified on SIP INVITE Messages	SIP INVITE messages are now validated. This helps detect invalid provisioning or configuration, as well as providing a basic check against intrusion from unauthorized call-agents. **Note** This is applicable to the CP environment only. An alarm is generated when an invalid SIP INVITE is detected due to an invalid domain name. The event is corrected with the following steps: 1. Verify the provisioned domain name and the one used by SIM to process the command-line parameter. 2. Verify the message source, whether it is on-net request or a potential unspoofed intrusion attempt. A "403 FORBIDDEN MSG" is returned in response to an "INVITE MSG" from an unauthorized/unrecognized CP. The CP processes the call as a basic call. Due to a change in the Logical IP Migration feature, this feature is suppressed by default in Release 4.5.x. To turn on the DOMAIN NAME validation feature, use the -enable_dnv option included in Args= of the platform.cfg for POTS and ASM.	
SIP Stack Attempts Next Address If TCP Connection Fails for INVITE	When provisioning a SIP trunk-grp, the SOFTSW_TSAP_ADDR is usually set to a FQDN that resolves to two or more IP addresses for the destination SIP endpoint(s). Prior to Release 4.5.x, when transmitting a SIP request, if the NON_SRV_TRANSPORT of the softsw-tg-profile is set to TCP and there is a failure to communicate with the first IP address of the FQDN, then no other IP address is tried. In Release 4.5.x, the software has been enhanced so that each of the IP addresses that the FQDN resolves to is tried in succession when there is a failure to communicate with the destination SIP endpoint. **Note** This functionality has always worked when UDP is the selected transport.	
SIA Authentication	This is an enhancement for efficient lookup while processing requests targeted for SIP subscribers. It involves internal caching of the Serving Domain Name of the user sending a SIP request and using it for subsequent messages instead of doing a separate table lookup for each request.	

Table 1-1 New Cisco BTS 10200 Softswitch-Based SIP Features

SIP Feature	Description	For More Information
SIP NOTIFY Rejected from Unity	In previous releases, if a request was received from a trunk that had the same domain name as the Cisco BTS 10200 serving domain name in the from header, the call failed, and the MWI Notify from Unity was rejected. This is resolved in Release 4.5.x. In Release 4.5.x, it performs the trunk identification before subscriber identification, and thus identifies the trunk correctly.	
Change Counter Names to SIS and SIP for Release 4.5.x Measurements	The PEG Counters names were changed to match industry terminology. There are two types of SIP counters, those used by multiple stacks related to SIP, and those used by the SIP Adapter. The Cisco BTS 10200 documentation uses the new names for several counters. In Release 4.5.x: 1. SIP common counters now begin with SIS_ instead of SIP_ for the SIA, SIM, POTS, and AIN categories. 2. SIA-specific counters now begin with SIA_ instead of SIP_. 3. AUDIT_SIP counters in the SIA category now begin with SIA_AUDIT instead.	

Table 1-2 lists the SIP subscriber features introduced in previous releases of 4.*x*.

Table 1-2 Cisco BTS 10200 Softswitch-Based SIP Features

SIP Feature	Acronym
Call forwarding deluxe activation	CWDA
Call forwarding deluxe deactivation	CWDD
Call forwarding deluxe interrogation	CWDI
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
Do Not Disturb activation	DND_ACT
Do Not Disturb deactivation	DND_DEACT
Anonymous call rejection activation	ACR_ACT
Anonymous call rejection deactivation	ACR_DEACT
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 barring interrogation	OCBI

Other Common Subscriber Features

Table 1-3 lists the most-commonly used existing subscriber features, some of which have been enhanced or modified for use by the Cisco BTS 10200 with the SIP protocol.

Note Table 1-3 lists the most commonly used Softswitch-based features; however, it is not an exhaustive list.

Table 1-3 Most Common Cisco BTS 10200 Softswitch-Based Features

Feature	Acronym
Activation and Deactivation of Anonymous Call Rejection	ACR
Billing	
Call Forwarding	CF
Calling Name and Number Delivery	CND
Caller ID Suppression	CIDS
Called Party Termination	CPT
Cisco BTS 10200 Supplementary Vertical Service Code Features	VSC
Customer Access Treatment	CAT
Customer-Originated Trace	COT
Direct Inward Dialing	DID
Direct Outward Dialing	DOD
Do Not Disturb	DND
Emergency Call	E911
E.164 and Centrex Dialing Plan (Extension Dialing)	E.164
Incoming and Outgoing Simulated Facility Group	ISFG and OSFG
Interworking	
Multiple Directory Numbers	MDN
Operator Services (0-, 0+, 01+, 00 Calls)	
Outgoing Call Barring	OCB
Remote Activation of Call Forwarding	RACF
SIP Endpoint Caveats	
SIP Subscriber to SIP Calls	
Type of Service	TOS

Phone-Based Features

Table 1-4 lists the phone-based features.

For more information about these features, see the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document.

.

Table 1-4 Phone-Based Features

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

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.

Jointly-Provided Features

Table 1-5 lists the most commonly used jointly-provided based features.

For more information about these features, see the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document.

Table 1-5 Jointly-Provided Features

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

SIP Trunk Features

The SIP Trunk features supported by Release 4.2 are listed in Table 1-6. For more information about the features, see Chapter 3, "SIP Protocol Trunk Features."

Table 1-6 SIP Trunk Features

Feature	Acronym
Call Redirection	
DNS SRV	
Type of Service	ToS
Reliable Provisional Responses	
Diversion Indication	
Carrier Identification Code over SIP	CIC
Number Portability Information over SIP	NP
Voice-Mail over SIP: Message Waiting Indication	MWI
Voice-Mail over SIP: Cisco BTS 10200 Centrex Subscribers	
SIP Trunk Sub-Groups	
Session Timer	
SIP-T	
DTMF SIP Signaling	
Asserted Identity	
Third-Party Call Control	3PCC
ANI-Based Routing	
TCP/UDP	
Business Group ID	BGID
Trunk Group ID	TGID

Limitations on Number of URLs, Parameters, and Headers (Release 4.5.1, Maintenance Release 2)

The system imposes limits on the decoding of incoming SIP messages. These limits are applicable to both subscriber-related and trunk-related incoming SIP messages. These limitations are intended to protect the system from decoding extremely large messages, which in turn could overload the system and cause performance problems.

Note These limits are not provisionable. If you need to change any of these limits, contact your Cisco account team.

Table 1-7 lists the limits related to URL and ReqUri.

Table 1-7 Limits on URL and ReqUri

Description	Limit
Maximum number of URLs (SIP+Tel+Unknown) in a SIP message	25
Maximum number of parameters in the ReqUri of a message	10
Maximum number of header parameters (parameters occurring after "?" character) in the Requset-URI of a message	5
Maximum number of parameters in a SIP URL	10
Maximum number of header parameters (parameters occurring after "?" character) in a SIP URL	5
Maximum number of parameters in a Tel URL	5

Table 1-8 lists the maximum number of parameters allowed in each type of SIP message header.

Table 1-8 Maximum Number of Parameters Allowed in SIP Message Headers

Header Name	Maximum Number of Parameters Allowed in Header
Contact	10
Via	10
Route	5
Record-Route	5
Diversion	10
Call-Info	5
Alert-Info	5
Error-Info	5
P-Asserted-Identity	5
Accept-Contact	5
To	5
From	5

Table 1-8 Maximum Number of Parameters Allowed in SIP Message Headers (continued)

Header Name	Maximum Number of Parameters Allowed in Header
Referred-By	5
Refer-To	5

Table 1-9 lists the maximum number of unknown Option tags of a specified kind in a SIP message.

Table 1-9 Maximum Number of Unknown Option Tags in SIP Message

Message	Maximum Number of Unknown Option Tags Allowed
Supported	5
Unsupported	5
Require	5

Table 1-10 lists the maximum number of parameters allowed in each type of SIP message header.

Table 1-10 Maximum Number of Parameters Allowed in SIP Message Headers

Header Name	Parameter Type	Maximum Number of Parameters Allowed in Header
Replaces	All parameters	5
Event	All parameters	5
Reason	All parameters	5
Accept	All parameters	5
Session-Expires	All parameters	5
Min-SE	All parameters	5
Warnings	All parameters	5
Accept-Language	Number of languages in the Accept-Language header	5
Accept-Language	Language parameters	5
Accept-Encoding	All parameters	5
Authorization	All parameters	15
Retry-After	All parameters	5

Table 1-11 lists the maximum number of headers allowed in a SIP message.

Table 1-11 Maximum Number of Headers Allowed in a SIP Message

Header Name	Maximum Number of Headers Allowed
Contact	5
Via	5
Route	5
Record-Route	5

Table 1-11 Maximum Number of Headers Allowed in a SIP Message (continued)

Header Name	Maximum Number of Headers Allowed
Diversion	5
Call-Info	5
Alert-Info	5
Error-Info	5
P-Asserted-Identity	5
Contact	5
To	1
From	1
Call-ID	1
CSeq	1
Session-Expires	1
Min-SE	1
Referred-By	1
Refer-To	1
Replaces	1
Allow-Events	5
Event	1
Reason	5
Accept	5
Accept-Encoding	5
Authorization	1
Retry-After	1

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:

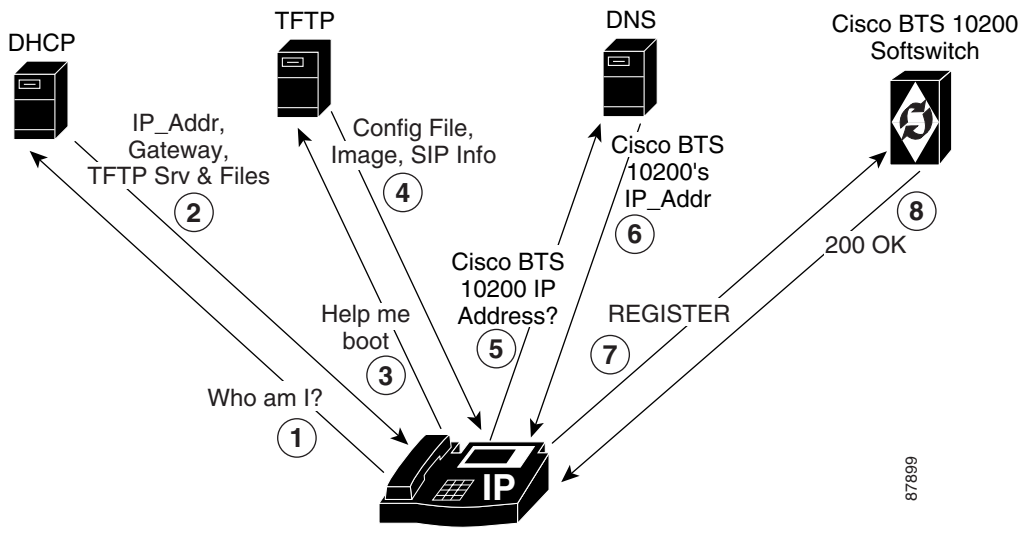
SIP Phone Initialization

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.

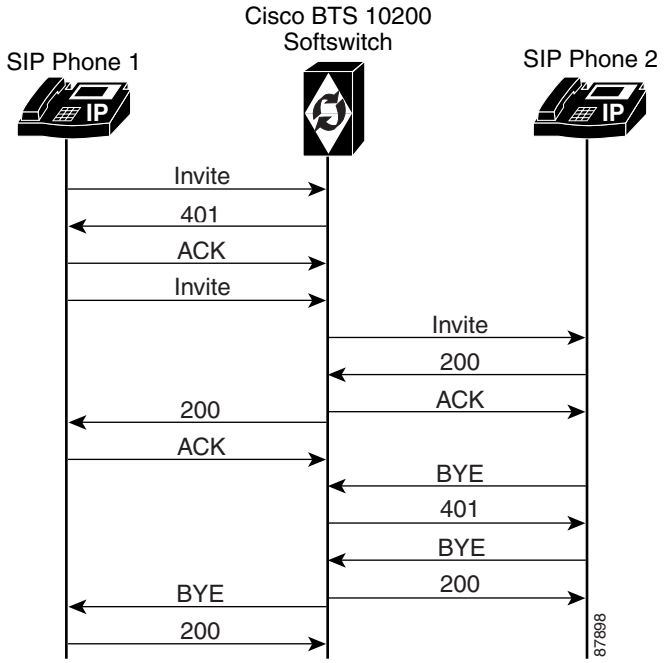
The following new tables have been defined for SIP subscribers, which are pertinent to Authentication:

- 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)



Cisco BTS 10200 Softswitch authenticates IP phones by using the MD5 digest defined in RFCs 3261 and 2617. The Cisco 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.

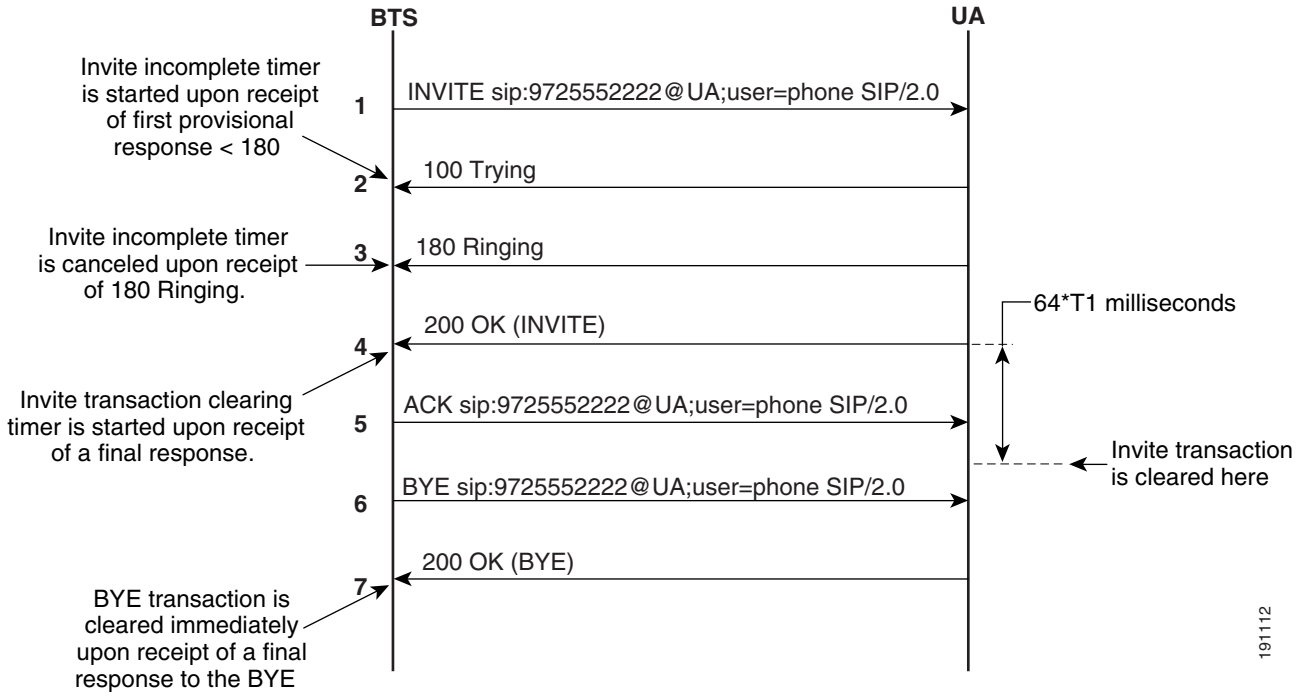
  When a BYE is subsequently sent or received on a call in progress, and timer I is running for that call, it is canceled and restarted for a smaller fixed duration of four seconds to reduce CCB hold time after call completion, and to optimize CCB resource usage.

- 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

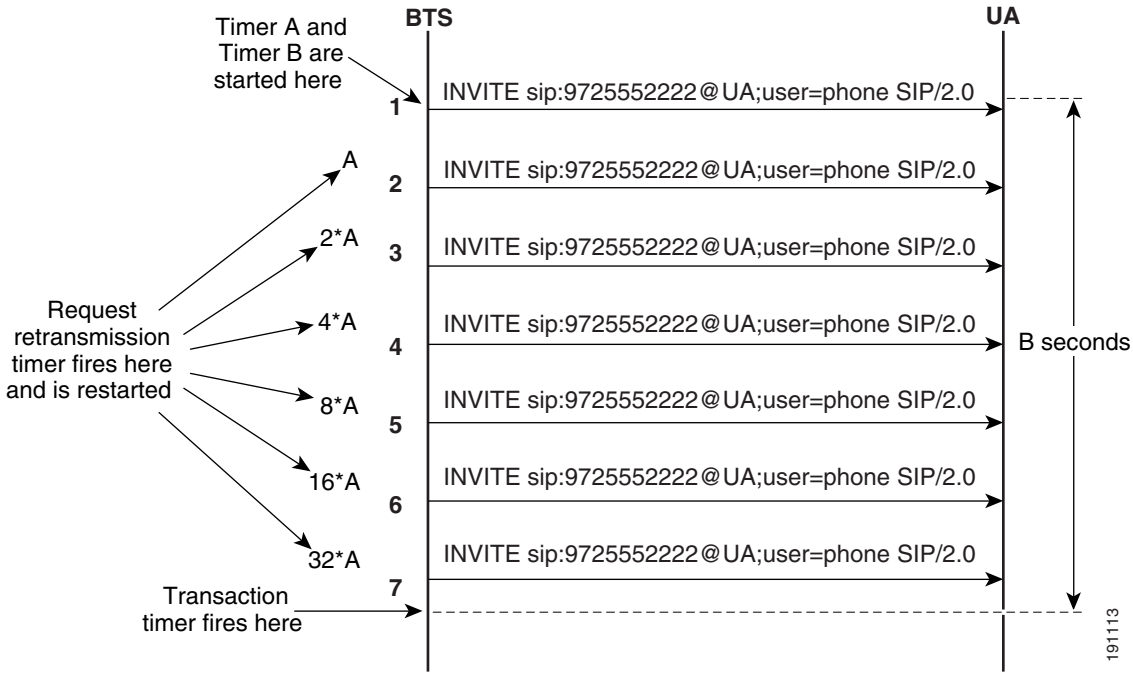
The retransmit count, or number of times the same request or response is retransmitted after the message is sent once to the transport layer, is computed based on RFC3261 recommendations.

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

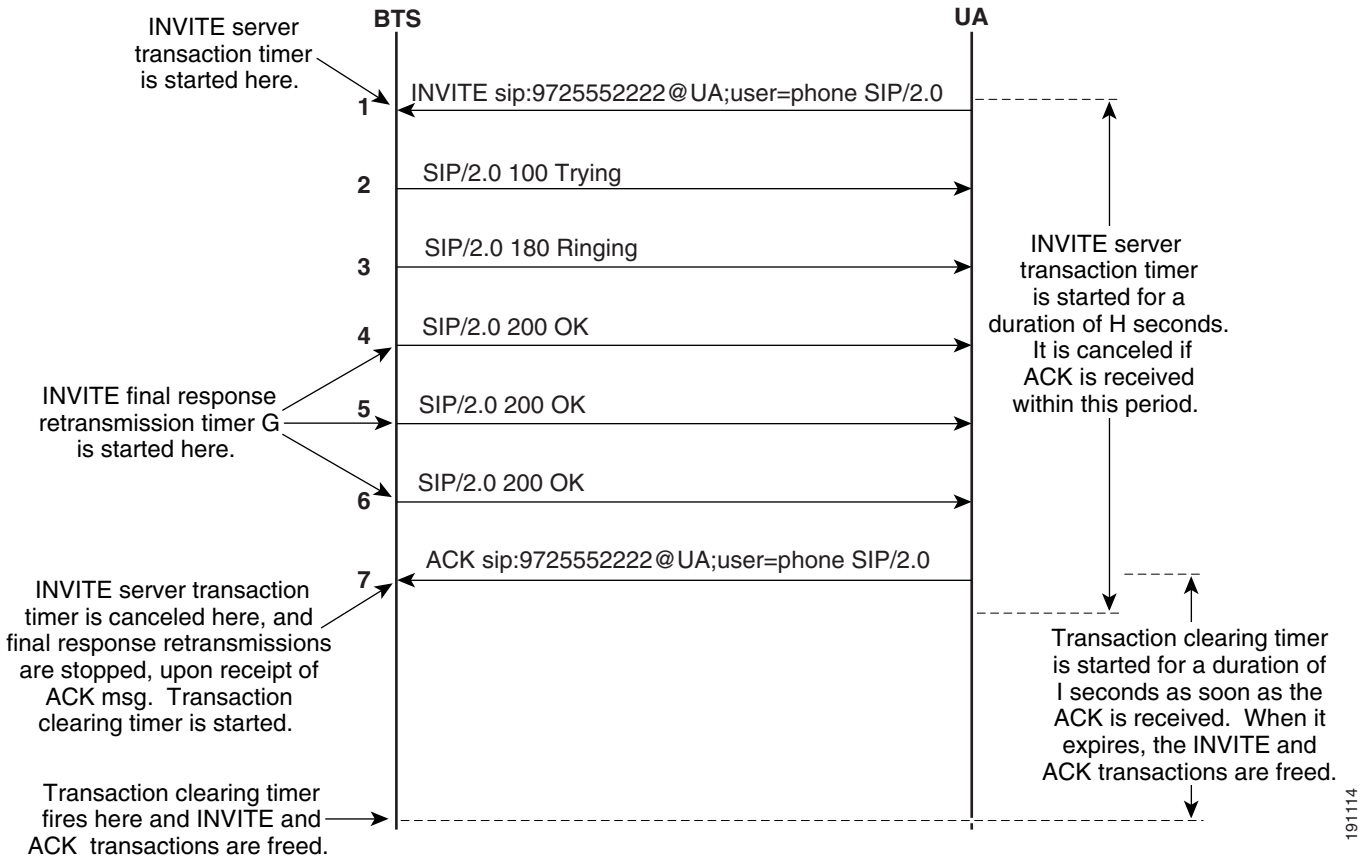
If there is no response for the initial non-INVITE request, then INIVTE requests are retransmitted as shown:

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.’

SIP Protocol Trunk Features

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

As the previous chapter described, Cisco BTS 10200 Release 4.5.x supports the SIP protocol by addressing two aspects of SIP: SIP subscribers and SIP trunks. This chapter encompasses SIP trunks.

The purpose of SIP trunks is to service SIP calls between Cisco BTS 10200 and external SIP entities other than local SIP subscribers, such as a voice-mail server, remote call agent or SIP proxy.

SIP Trunk Properties

Cisco BTS 10200 can be configured to use UDP or TCP transport for communications over a SIP trunk. A SIP trunk is configured in Cisco BTS 10200 with the following:

- IP address or Fully Qualified Domain Name (FQDN) and port for address information of external SIP entity.
- Dial plan and dialed digit string entries for routing.
- Profile to define the feature set for a SIP trunk.

SIP Trunk Characteristics

SIP trunk characteristics include the following:

- Typically, one trunk is defined for each external SIP entity communicating with Cisco BTS 10200 over SIP.
- Multiple trunks can be associated to a provisioned route set providing “route advance” functionality.
- SIP trunks have OAM state and status, and can be set “in service” and “out of service” by the administrator.
- SIP trunks currently will not set themselves “out of service” if the remote SIP entity does not respond.
- Trunks can be defined as one of three possible trunk types: SIP, SIP-T and CMSS.
- External SIP entities are addressed as follows:
  - SIP-T trunk must communicate with Cisco BTS 10200 using the SIP-T protocol.
  - CMSS trunk must communicate with Cisco BTS 10200 using the PacketCable CMSS specification (partially supported in Release 4.5.x).

  - SIP trunk must communicate with Cisco BTS 10200 using standard SIP protocol.
- A regular SIP call may be received on a SIP-T trunk.
- Multiple trunks can be defined to the same external SIP entity IP address and port, using the BGID/TGID SIP trunk feature.

Outbound Cisco BTS 10200 SIP Call

Inbound calls on Cisco BTS 10200 are processed by the Cisco BTS 10200 routing system. The routing system selects an outbound SIP trunk based on the digits dialed and dial plan of the originating entity. The SIP call is then transmitted out a TCP or UDP socket toward the IP address associated to the trunk selected by routing. SIP call features and characteristics are applied to the outbound call based on the feature selections in the trunk profile associated with the trunk.

RFC 3398 states that any outbound SIP number with NOA of NATIONAL must be prefixed with "+CCnumber" which is an international format, and any number with NOA=subscriber must be formatted also with international significance. The sending of the full E.164 format is enabled by a flag (send-full-e164) in the softsw-tg-profile table to enable interworking with downstream devices that require this number format.

Inbound Cisco BTS 10200 SIP Call

For inbound calls, the SIP call is received on a TCP or UDP socket. The Cisco BTS 10200 determines which SIP trunk the call is associated with, by comparing the address of the previous hop SIP entity in the VIA header of a request, with the IP addresses associated with the provisioned SIP trunks, for a match.

If the previous hop SIP entity is represented by an FQDN, then Cisco BTS 10200 compares it against SIP trunks associated to this FQDN. If the SIP call is not associated to any trunk, the call is refused, unless of course it is identified to be from a local Cisco BTS 10200 subscriber.

The SIP call is then sent to the routing system with the trunk identification. The routing system uses the dial plan associated with the inbound trunk and the dialed digits to make routing decisions for the outbound direction.

SIP Trunk Features

- Session Timers
- SIP Timer Values
- SIP-T, ISUP Version, ISUP-Transparency, and GTD
- DTMF SIP Signaling
- Asserted Identity and User-Level Privacy
- Third-Party Call Control
- ANI-Based Routing
- Trunk Group Audit for the SIP Adapter
- T.38 Fax Relay Call Agent Controlled Mode Across SIP Trunk Interface

Validation of Source IP Address for Incoming SIP Messages (Release 4.5.1, Maintenance Release 1)

The system is capable of performing source IP address validation of incoming messages received on SIP trunks. This validation process is intended to reduce the risk of security attacks, which can occur if a packet is sniffed in the network and then sent from a different or rogue IP address, or domain, as present in the Via header. By default, IP address validation is disabled on the Cisco BTS 10200 Softswitch. The service provider can enable this capability using the SIA-TG-VALIDATE-SOURCE-IP token in the ca-config table. This is a switch-wide parameter, and applies to all SIP trunk groups.

Provisioning details can be found in the Chapter 2 of the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

Hop Counter and Maximum Forwards Parameters

The system supports provisionable parameters in the softsw-tg-table that allow control of the maximum-forwards and hop-counter fields of the SIP Invite message:

- HOP-COUNTER-MAX
- HOP-COUNTER-SUPP
- MAX-FORWARDS
- SCALE-FACTOR

Note The hop count between SIP and SS7 networks is scaled appropriately in the Cisco BTS 10200 Softswitch based on the provisioning of the SCALE-FACTOR token.

The description and relationship of these parameters are provided in the "Softswitch Trunk Group Profile" section on page 5-2.

Call Redirection

Call Redirection allows a remote SIP endpoint receiving a call from the Cisco BTS 10200 to re-route the call back on the Cisco BTS 10200, using one or more destinations provided by the endpoint. It also supports load sharing and redundancy solutions used by other switches or applications interworking with Cisco BTS 10200 using SIP. These solutions typically involve a front-end SIP network management server to manage load sharing and redundancy for back-end servers.

The Cisco BTS 10200 honors the redirection (SIP 300 class) response to a SIP INVITE call request, and redirects the call using the specifications outlined in RFC 3261. The Cisco BTS 10200 Softswitch does not support sending a redirection response.

When a redirection response is received with multiple contacts, multiple redirections are attempted in serial in the order the contacts were received. This includes contacts received in subsequent redirection responses, in which case the contacts are appended to the serial list of redirections being attempted. Redirections are attempted up to a provisioned limit at which point Cisco BTS 10200 releases the call. There is also a provisioned limit to the number of 300 class responses received for any given call.

Cisco BTS 10200 requires redirection contacts to have a SIP URL format. The user information field of the SIP URL must be present and contain a numeric phone number and a host name. The following example illustrates the SIP URI format:

```
sip:2125553333@phone.cisco.com
```

Call redirection is not supported on SIP trunks provisioned with a business group. Cisco BTS 10200 does not support an incoming 300 class response from a local Cisco BTS 10200 SIP subscriber.

When the Cisco BTS 10200 selects a contact from the 300 class redirection response to perform a call redirection, it decides how the redirection is done based on the number and host name in the contact's SIP URL. If the host name is the same as the configured SIP contact, the Cisco BTS 10200 routes the call using the number in the user portion of the redirected contact URL. If this number also matches the called number in the redirected INVITE, then the Cisco BTS 10200 routes by advancing to the next trunk in the provisioned route set. This is called "route-advance." If this number does not match the previously called number, the Cisco BTS 10200 determines the next trunk to send the call out by performing routing on the new number. This is called a "reroute."

Note A provisionable parameter allows the service provider to force the system to use the reroute method regardless of whether the redirect number matches the number in the initial INVITE. This parameter is part of the call agent configuration and affects all SIP trunks on the switch.

If the host name field of the redirection contact selected for call redirection matches the provisioned TSAP address of a provisioned Cisco BTS 10200 SIP trunk, the Cisco BTS 10200 redirects the call out this trunk without going through the Cisco BTS 10200 routing system. The number in the contact is set as the called party number in the Request URI of the redirected INVITE.

If the host name field does not match the SIP contact of the Cisco BTS 10200 or the TSAP address of any of the provisioned SIP trunks, then the call is redirected toward the host identified in the contact UR. This contact URI is used as the request URL for the redirected call. The redirected call uses the properties of the SIP trunk in the previous call attempt, and the call does not go through the Cisco BTS 10200 routing system. However, if the profile of this SIP trunk restricts redirection to contacts having host names matching only SIP trunks or Cisco BTS 10200 contact, then redirection is not performed for this contact.

If the diversion feature is enabled for the Cisco BTS 10200 SIP trunk selected for call redirection, and the last redirection response received contained diversion headers, these headers are populated in the newly redirected call. This follows the diversion rules.

With call redirection, users can provision a limit on the maximum number of 300 class redirection responses the Cisco BTS 10200 accepts while performing redirection on any given call attempt; the default is 1. The feature also allows a user provisioned limit for the maximum number of actual call redirection attempts the Cisco BTS 10200 makes on any given call attempt; the default is 5. These provisioning parameters are part of the call agent configuration and apply to all SIP trunks.

Users can enable or disable call redirection for any provisioned SIP trunk. By default, call is enabled to accept contacts only with host names of the Cisco BTS 10200 SIP contact, or the TSAP address of any provisioned SIP trunks. This provisioning parameter is part of the Softswitch trunk group profile.

Provisioning details for call redirection can be found in the Call Redirection section in Chapter 2 of the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

Locating SIP Servers Using DNS Queries

This section explains how the system locates SIP servers, which it can do by either of the following methods:

- Using information from an incoming request.
- Using the SIP trunk provisioning in the database.

Locating SIP Servers from an Incoming Request

The Cisco BTS 10200 Softswitch can request and accept TCP connections. The system provides for the selection of TCP or UDP on trunk groups with or without SRV support. When accepting connections, the Cisco BTS 10200 Softswitch listens for and accepts TCP connection requests. It also listens for incoming requests on UDP. Once a request is received, the system sends SIP responses using the same transport type as the associated request. If this occurs over a TCP connection and the connection still exists, the system reuses that connection. If the connection is gone, the system attempts to establish a new connection to the same address.

Locating SIP Servers from an Outbound Request

The NAPTR and SRV DNS functions allow the Cisco BTS 10200 Softswitch SIP interface to correctly interoperate with proxy farms and find proxies and redirect servers. Operators can designate some service hosts as primary servers, and others as backup. When provisioned to support NAPTR and SRV functions, the Cisco BTS 10200 Softswitch discovers the most preferred transport protocol of the locally supported destination, and obtains an SRV query string to locate a server supporting that protocol. The system follows the procedures described in RFC2782 and RFC3263 to determine the transport, IP address, and port for the next hop.

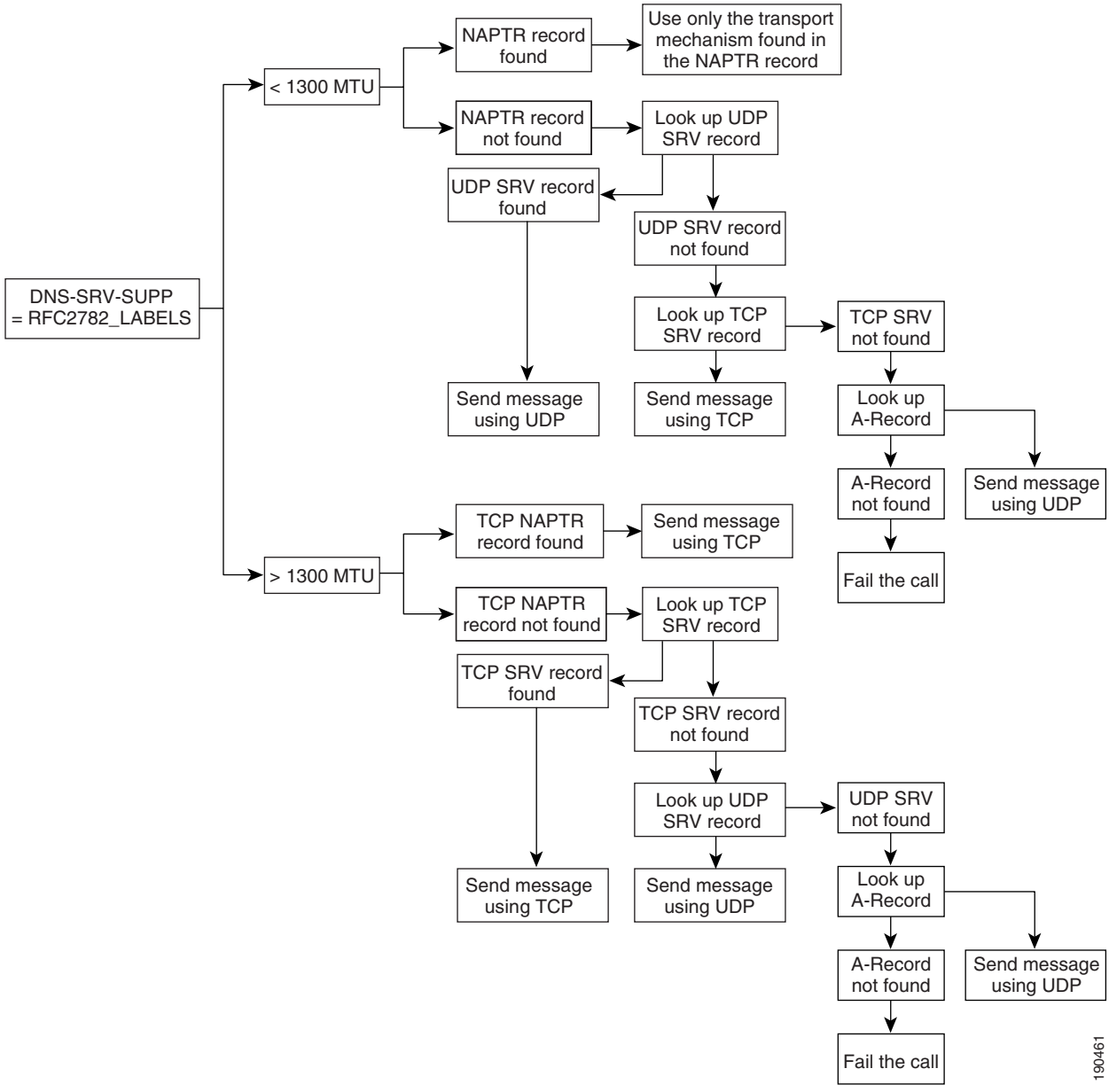
Note To provision NAPTR and SRV support, set the DNS-SRV-SUPP field in the SOFTSW-TG-PROFILE table to RFC2782_LABELS.

The NAPTR lookup procedure depends on the size of the message compared to the path maximum transmission unit (MTU) size stated in RFC3261 and RFC3263 (typically 1300 bytes). The implementation in the Cisco BTS 10200 Softswitch is based on the SIP Working Group Document

Issue 760 (http://bugs.sipit.net/show_bug.cgi?id=760). That document provides guidance regarding the conflicting directives between RFC3261 and RFC3263 when a message size exceeds the MTU limit and NAPTR lookups are involved. The system processes the lookup as described in this section.

Figure 3-1 shows the transport selection procedure for sending SIP requests based on NAPTR and SRV records, that is, when the value of the DNS-SRV-SUPP token is provisioned as RFC2782_LABELS.

Figure 3-1 Transport Selection for Sending SIP Requests Based on NAPTR and SRV



Following is an explanation of the logic shown in Figure 3-1.

- If the message size is less than the path MTU limit, the sequence is as follows:

a. The system looks up a NAPTR record, and chooses a transport protocol based on the priority of the NAPTR record. Only that chosen transport protocol is used to route the message, and servers associated with other protocols are not contacted.

b. If no NAPTR record is found, the system performs a best-effort lookup by assuming that an SRV record exists that has the same name as the NAPTR record. The procedure continues as follows:

– A UDP SRV record is looked up first, using the _sip._udp prefix. If it is resolved, the servers on the resulting list are contacted and UDP transport is used to send the message.

– If no UDP SRV record is found, a TCP SRV record is searched, using the _sip._tcp prefix. If it is resolved, the servers on the resulting list are contacted and TCP transport is used to send the message.

- If the message size is greater than the path MTU limit, the sequence is as follows:

a. The system performs a NAPTR lookup for records supporting TCP transport only. The resulting query string from the NAPTR lookup is used to perform an SRV lookup. If it is resolved, the servers on the resulting list are contacted and TCP transport is used to send the message.

b. If no NAPTR record is found, the system performs a best-effort lookup by assuming that an SRV record exists. the procedure continues as follows:

– A locally generated query string is used to query SRV records, using TCP as preferred transport and the _sip._tcp prefix. If such a record is found, servers on the resulting list are contacted and TCP transport is used to send the message.

– If no TCP SRV record is found, a UDP SRV record for the same TSAP address (prefixed with _sip._udp) is searched. If such a record is found, all servers on the resulting list are contacted and UDP transport is used to send the message.

The following details apply to all DNS queries described above:

- The above procedure (selecting only a single transport) applies only to NAPTR or SRV provisioning, that is, when the following are both true:
  – The SIP trunk profile is provisioned with SRV support enabled.
  – The TSAP address is provisioned with either a NAPTR or SRV name.
- After the system selects a transport type, only that type is used for signaling. If the chosen transport does not work, the system does not attempt any other transport mechanism, and the call fails.
- If the NAPTR and SRV queries fail, the system attempts a best-effort A-record query and uses UDP to send the message.

Tip These steps add overhead to the process of resolving an address. Therefore, SRV should only be enabled if the benefits of the address resolution procedure are required.

Traversing the SRV List for Failure Responses and Retransmission Timeouts

This section describes how the Cisco BTS 10200 Softswitch traverses the SRV list.

- 503 Response—When the Cisco BTS 10200 Softswitch receives a 503 response (service unavailable) from the server in the SRV list that was last attempted, it resubmits the same request as a new transaction (with a new branch ID) to the next IP address in the SRV list.

- Retransmission timer expires—If an SRV server receiving the INVITE does not respond within the retransmission timer period, the Cisco BTS 10200 Softswitch can send the next retransmission of the same request to the same server (as recommended in RFC3263), or to the next server in the SRV list (legacy Cisco BTS 10200 Softswitch behavior). This is controlled using a provisionable flag, DNS_SRV_ADV_ON_RETRANS_TIMEOUT on the SOFTSW-TG-PROFILE table:
  - If DNS_SRV_ADV_ON_RETRANS_TIMEOUT is set to N, all retransmissions of a message are exhausted sending to a single address before attempting to send to the next address. Keep in mind that some calls may not complete if one of the nodes in an SRV list returns a 503 message, even though other nodes in the list are capable of handling the request successfully.
  - If it is set to Y (the default value), the system retransmits the same request as a new transaction (with a new branch ID) to the next IP address in the SRV list.

A-Record DNS Queries for Outgoing Messages

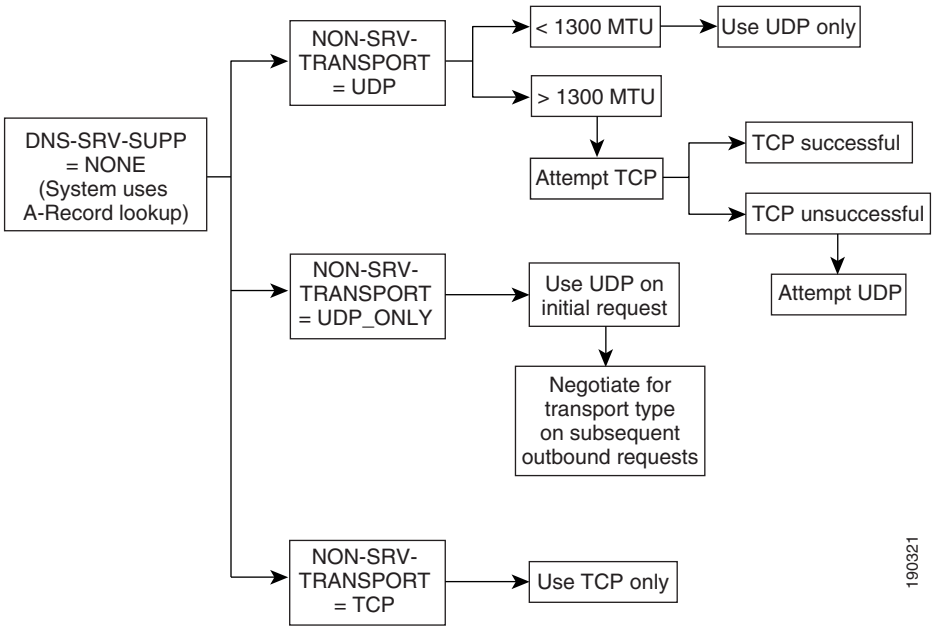
The system can use A-record DNS queries to locate SIP servers. The system selects this DNS query and the transport mechanism based on the value of the DNS-SRV-SUPP field in the SOFTSW-TG-PROFILE table. If this field is set to NONE, the transport is selected based on the NON-SRV-TRANSPORT field of the SOFTSW-TG-PROFILE table. Possible values for this field are as follows:

- UDP (default)—If the message size is less than 1300 bytes as described in RFC 3261 and RFC 3263, the system uses UDP. If the message size is greater than 1300 bytes, the system uses TCP; however, if TCP fails, the system attempts to use UDP.
- UDP-ONLY—The initial outbound request uses UDP regardless of the message size. However, the transport used for subsequent outbound requests is based on the negotiated transport type exchanged in the Contact: header during dialog establishment.
- TCP—Use TCP only.

When performing an A-record DNS query, the system tries each IP address to which the FQDN resolves, (in succession) when there is a failure to communicate with the destination SIP endpoint. The system does this for both UDP and TCP transport mechanisms.

Figure 3-2 shows the transport selection procedure for sending SIP requests based on A-Record queries, that is, when the value of the DNS-SRV-SUPP token is provisioned as NONE.

Figure 3-2 Transport Selection for Sending SIP Requests Based on A-Record Lookup



Provisioning Commands

To provision the parameters in the SIP trunk that affect DNS query procedures, see the DNS query provisioning procedure in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

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.

Users can set the ToS value on a system-wide basis or on a per trunk group basis. The policy is selected in the call agent configuration. If system-wide ToS is selected, the ToS value is also specified in the call agent configuration.

The default SIP ToS value for system level ToS selection is as follows:

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

Note Cisco does not recommend using any value other than the specified default. Changing the value from its default may significantly impact network performance. Consult Cisco support for assistance.

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.

If Cisco BTS 10200 cannot read the SIP ToS configuration values from the call agent configuration, it initializes the ToS level to the default and selects the system level ToS policy.

If SIA-TRUNK-GRP-LEVEL-SIG-TOS is set to Y in the call agent configuration, Cisco BTS 10200 uses the trunk group's ToS level for every message sent on the trunk group. If any message is sent out to any endpoint other than a provisioned trunk group, the system level ToS is used.

Alternately, Cisco BTS 10200 can be provisioned to use the SIP trunk's provisioned ToS level for every SIP message sent out a particular SIP trunk. The system level ToS is used for SIP messages sent out to the Cisco BTS 10200 local SIP subscriber endpoints.

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 across Cisco BTS 10200 SIP trunks.

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, refer to the 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.

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 on a BTS 10200 SIP trunk with the diversion feature enabled, 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. A BGID is added to a diversion header as a token parameter if the feature for business group identification is enabled, and the diversion number is in a Centrex format.
- For Release 4.5.1, Maintenance Release 2 and later—Privacy parameters are sent and received in the Diversion header.

For INVITEs received on a SIP trunk with the diversion feature enabled, the following behaviors apply:

- If no diversion headers are present in the incoming message, no diversion information is identified.
- If exactly one diversion header is present in the incoming message, the number in the diversion header is identified as the ‘original called’ party number. The diversion ‘reason’ and ‘count’ are also interpreted.
- If more than one diversion headers are present in the incoming message, the bottom-most diversion header determines the ‘original called’ number. The top-most diversion header determines the ‘last forwarding’ party and diversion reason. The total diversion count is determined by the summation of the diversion counter values across all the diversion headers received. The rest of the diversion information is ignored.
- If the diversion feature is disabled and diversion headers are present, the diversion headers do not determine diversion information for call processing. They are ignored.
- If the diversion feature is disabled on a provisioned SIP-T trunk, and the trunk receives a call on that trunk with an INVITE number in the ‘To:’ field that differs from the Request URL number, then the ‘To:’ field number is interpreted as the ‘original called’ number. Any diversion headers present are ignored.

Users can enable or disable diversion indication for a provisioned SIP trunk in the softswitch trunk group profile table; the feature is disabled by default. For provisioning details, see the “Diversion Indication” section in the *SIP Protocol Provisioning Guide*.

Carrier Identification Code over SIP

Support for the carrier identification code (CIC) over SIP allows a SIP to PSTN gateway entity receiving a call to determine which carrier the originator prefers to handle the call. This parameter value may indicate which long distance carrier the originator has subscribed to handle the call.

Cisco BTS 10200 support for this feature follows the specifications described in the IETF draft ‘draft-yu-tel-url-07.’ Support for CIC is limited to local CIC formats. Global CIC formats, which use country code, are not supported. If a global CIC is received, the global part is ignored and the call is processed using the local portion.

For calls sent out over a Cisco BTS 10200 SIP trunk, the CIC, when available, can be added as a parameter of the user portion of the Request URI of the outgoing INVITE message. The CIC value is derived either from the subscriber record, in the case of local subscriber originated call, or from the 'transit-network-select' information if the call was received from a PSTN origination. The option to send the CIC parameter on the outbound SIP trunk is provisioned using the send-cic-param token in the softsw-tg-profile table.

For calls received on a Cisco BTS 10200 SIP trunk, if the CIC parameter is present in the received SIP INVITE then the value of the CIC is identified for call processing. If the CIC was received in global format, the country code component of the CIC is ignored.

For local Cisco BTS 10200 subscribers, the CIC is provisioned in the subscriber record.

Number Portability Information over SIP

Number portability (NP) allows a subscriber to move geographically within the network domain without requiring a change to the subscriber's phone number. NP information is sent with the initial SIP INVITE message. The information indicates to the receiving switch if a previous switch has performed a database query to get routing information of the terminating subscriber. If the terminating subscriber has moved, the NP information routing number (RN) indicates the destination switch the terminating subscriber has moved to.

Cisco BTS 10200 support for this feature follows the specifications described in the IETF draft 'draft-yu-tel-url-07.'

For calls sent out a Cisco BTS 10200 SIP trunk, the NP information is added as parameters in the user portion of the Request URL of the outgoing INVITE message. A number portability dip indication (NPDI) flag is added to indicate a database query for NP information was performed, and the routing number (RN) parameter value pair is added to indicate the switch the terminating subscriber has moved to.

For calls received on a Cisco BTS 10200 SIP trunk, if the NPDI and RN parameters are present in the received SIP INVITE, then this NP information is identified for call processing.

The signal ported number flag in the trunk group configuration enables or disables the population of NP information for SIP calls sent out a SIP trunk. The default is to send NP information on the outgoing SIP call if the information is available. If NP information is included for an incoming call, the information is used in call processing regardless of the provisioned flag setting. For provisioning details, refer to the provisioning guide.

SIP Trunk Subgroups

Multiple SIP trunk groups may be provisioned toward a single SIP endpoint (same IP address and port destination) differing only by a trunk subgroup identifier. Calls sent or received on these SIP sub-trunk groups contain the trunk subgroup identifier in the SIP request message identifying the trunk group.

Remote SIP servers or switches requiring additional network-specific or application-specific properties for calls to and from Cisco BTS 10200 use the SIP trunk subgroups feature. A remote SIP entity may require Cisco BTS 10200 to identify from which call rate center a call originated. A SIP trunk subgroup may be provisioned to represent one of the rate centers. Each trunk has a unique subgroup identifier. Routing tables can be configured to select the trunk that represents the rate center, and the calls sent out the SIP trunk then include the unique rate center identifier.

For any INVITE sent out a SIP trunk subgroup by Cisco BTS 10200, a Cisco BTS 10200 proprietary SIP URL parameter 'tgid' is added to the request URI. The 'tgid' value is retrieved from the SIP trunk subgroup the call is sent out on.

An example of this parameter syntax follows:

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

When the Cisco BTS 10200 Softswitch receives a call on a SIP trunk subgroup from a remote SIP endpoint, the endpoint is required to send the 'tgid' parameter to identify the trunk subgroup. The value must match one of the provisioned trunk subgroups. The 'tgid' type is specified in the trunk-sub-grp-type field in the softsw-tg-profile table, and the 'tgid' value is provisioned in the trunk-sub-grp field of the trunk-grp table.

Note The ‘bgid’ and ‘tgid’ parameters are mutually exclusive. Only one can be enabled on a trunk.

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. 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.

This SIP extension allows for a periodic refresh of SIP sessions using 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 the session timer follows 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. This feature does not require the session timer capability on the remote SIP endpoint.

If the Cisco BTS 10200 call agent switches over during an active call with a session timer active, the session timer is deactivated. In this scenario, if the Cisco BTS 10200 were the negotiated refresher of the session timer, a call release may occur on expiration of the session timer.

Users can enable or disable the session timer feature for a provisioned SIP trunk; the feature is disabled by default. The session timer is enabled by means of the session-timer allowed flag in the Softswitch Trunk Group profile.

When the session timer is enabled on the SIP trunk and an initial INVITE is sent by Cisco BTS 10200, a Supported header with a ‘timer’ value is added, as is a Session-Expires header with Refresher parameter set to ‘Uac’. Whenever the SIP call is sent from a Cisco BTS 10200 SIP trunk, Cisco BTS 10200 sets 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 by Cisco BTS 10200 at half of the negotiated Session-Expires value.

When this feature is enabled on the SIP trunk and an initial INVITE is received by 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 the 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 on the SIP trunk 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 trunk 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 trunk 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

For information on enhancements made to the SIP timers in Release 4.5.x, see the "SIP Timer Values" section on page 2-23.

SIP-T, ISUP Version, ISUP-Transparency, and GTD

SIP-T provides a standard for SIP to PSTN interworking. It provides seamless bridging between two PSTN networks by encapsulating ISUP information as a binary (non-GTD type) or textual (GTD type) SIP attachment body. It also provides the standard to interwork a SIP network with the PSTN by specifying the SIP header translation for SIP-PSTN gateways.

Cisco BTS 10200 support for SIP-T follows the specifications described in RFC 3372, RFC 3398, and RFC 3204. For details on how call signaling information elements are mapped between a SIP-T message (headers and encapsulated ISUP) and an SS7/ISDN message, contact your Cisco account team.

SIP-T ISUP formats supported by the Cisco BTS 10200 include GTD, Q761_HONGKONG (ITU), and ANSI GR-317. These values are provisioned using the SIPT-ISUP-VER field in the softsw-tg-profile (SIP trunk group profile) table. When a SIP-T message is sent out from the Cisco BTS 10200, it always indicates to the receiver that handling the ISUP is optional using the SIP content disposition header. A SIP-T call is refused if an initial INVITE is received with an unsupported ISUP version attached, and the message indicates that ISUP handling is not optional. If the ISUP handling was optional, the call proceeds by ignoring the ISUP information.

A SIP-T trunk is provisioned by setting the protocol type to SIP-T, and specifying one of the supported ISUP versions in the SIP trunk profile. When the system sends a SIP-T message with encapsulated ISUP, the SIP-T trunk sends the ISUP version, and the version label is set to the one provisioned. If there is a custom alias name for that version, the alias name is used in the message instead of the version label. This is accomplished by provisioning the SIPT-ISUP-VER-ALIAS table. The base parameter in the

message is set according to RFC 3204 in line with the version chosen. Since the base is optional, it may be removed from the SIP INVITE message using provisioning. Note that the GTD type does not include a base parameter regardless.

The provisioning system for defining a SIP-T trunk imposes the rule that the reliable provisional response feature is enabled.

The system supports ISUP versions applicable to SIP-T and SIP-GTD. To provision these parameters, see the "SIP-T, ISUP Version, ISUP-Transparency, and GTD" section in the *SIP Protocol Provisioning Guide*.

Note GTD parameters can be used to support ISUP transparency between the Cisco BTS 10200 Softswitch and the Cisco PSTN Gateway (PGW) 2200. For more information on provisioning this feature, see the "ISUP Transparency on the BTS-PGW Interface" section in the *Cisco BTS 10200 Softswitch Provisioning Guide*. For a description of this feature, see the "ISUP Transparency with the Cisco PGW 2200" section in the *Cisco BTS 10200 Softswitch System Description*.

DTMF SIP Signaling

This section provides the following information about DTMF SIP signaling:

- Feature Description
- Exceptions and Limitations

Feature Description

DTMF SIP signaling allows a remote SIP endpoint to receive SIP notifications from a Cisco BTS 10200 SIP trunk when a Cisco BTS 10200 local subscriber presses a DTMF digit on the handset during a SIP call. This notification identifies which digit was pressed, and for how long it was pressed. DTMF SIP signaling is used when a remote SIP endpoint requires DTMF notifications to drive interactive voice response (IVR) applications, and the DTMF notification information cannot be sent using the bearer path.

This feature sends DTMF notifications via SIP INFO or NOTIFY request messages from the Cisco BTS 10200 SIP trunk. The NOTIFY mechanism of delivering DTMF digits follows the mechanism described in draft-mahy-sip-signaled-digits-00.txt.

The remote SIP endpoint generic uses the SUBSCRIBE/NOTIFY mechanism to subscribe to the Cisco BTS 10200 SIP interface for telephone-event notifications. The mechanism is described in 'draft-roach-sip-subscribe-notify-03.' Alternatively, the SIP INFO method for notification of telephone events may be used for unsolicited notifications. Cisco BTS 10200 only sends DTMF notifications out SIP trunks. It does not support receiving notifications. Users can enable or disable the DTMF SIP signaling feature for a provisioned SIP trunk and the feature is disabled by default.

DTMF notifications are sent using the SIP INFO or NOTIFY request method, depending on the provisioning selection for the feature. The notifications are only sent within an active SIP call dialog.

If the INFO method is selected, Cisco BTS 10200 sends an INFO message once for each digit pressed. These messages are delivered to the contact address if Cisco BTS 10200 received the original INVITE, or to the initial INVITE's Request URI if Cisco BTS 10200 originated the call. The remote SIP endpoint must respond with a 200 response. The INFO method is specified in RFC 2976.

The following is an example of an INFO message sent from Cisco BTS 10200 when a subscriber has pressed the DTMF digit '1' for 250 milliseconds:

```
INFO sip:subscriber@remoteDomain.com SIP/2.0
Via: SIP/2.0/UDP bts.cisco.com:5060
From: Notifier <sip:notifier@bts.cisco.com>;tag=bts-1234
To: Subscriber <sip:subscriber@remoteDomain.com>;tag=1234-ABCD
Call-ID: 12345@bts.cisco.com
CSeq: 102 INFO
Content-Type: application/dtmf-relay
Content-Length: 22
Signal=1
Duration=250
```

If the Notify method is selected for this feature, the Cisco BTS 10200 sends two notify requests each time a DTMF button is pressed, once when the digit is pressed and once when the button is released. However, the feature does not send or buffer notifications during the SIP call unless the remote SIP endpoint has subscribed for these notifications during an active SIP call. DTMF notifications are sent over SIP during an active subscription until the subscription expires. A subscription expires if the call is released or if the subscription is not refreshed (re-subscribed) before its specified subscription duration. Either side may send indication of subscription expiry if an error occurred.

The following is an example of a subscription received on a Cisco BTS 10200 SIP trunk. In the example, the subscriber requests all telephone events that occur longer than 2000 milliseconds. The duration of the subscription requested is 1 hour (3600 seconds):

```
SUBSCRIBE sip:notifier@bts.cisco.com SIP/2.0
Via: SIP/2.0/UDP vocaldata.com:5060
From: Subscriber <sip:subscriber@vocaldata.com>;tag=1234-ABCD
To: Notifier <sip:notifier@bts.cisco.com>;tag=bts-1234
Call-ID: 12345@bts.cisco.com
CSeq: 102 SUBSCRIBE
Contact: Subscriber <sip:subscriber@vocaldata.com>
Event: telephone-event;duration=2000
Expires: 3600
Content-Length: 0
```

A 200 OK response is immediately sent from the Cisco BTS 10200 for the SUBSCRIBE, indicating the SUBSCRIBE message was received. The Cisco BTS 10200 sends an Expires header in this response to indicate what the subscription duration actually is. It may choose to reduce the subscription interval.

An initial NOTIFY is immediately sent to the remote endpoint, as soon as the subscription is created or refreshed. The following is an example this initial notify request:

```
NOTIFY sip:subscriber@vocaldata.com SIP/2.0
Via: SIP/2.0/UDP bts.cisco.com:5060
From: Notifier <sip:notifier@bts.cisco.com>;tag=bts-1234
To: Subscriber <sip:subscriber@vocaldata.com>;tag=1234-ABCD
Call-ID: 12345@bts.cisco.com
CSeq: 103 NOTIFY
Contact: Notifier <sip:notifier@bts.cisco.com>
Event: telephone-event;rate=1000
Content-Type: audio/telephone-event
Content-Length: 0
```

When an event is notified to the endpoint using the Notify request method, two Notify requests are sent indicating the beginning and end of the DTMF digit pressed. Each request contains the digit pressed and the duration in an encoded bit-mask. An example or this request follows. Consult the DTMF draft for the format of the bit-mask:

```
NOTIFY sip:subscriber@vocaldata.com SIP/2.0
Via: SIP/2.0/UDP bts.cisco.com:5060
From: Notifier <sip:notifier@bts.cisco.com>;tag=bts-1234
```

```
To: Subscriber <sip:subscriber@vocaldata.com>;tag=1234-ABCD
Call-ID: 12345@bts.cisco.com
CSeq: 104 NOTIFY
Contact: Notifier <sip:notifier@bts.cisco.com>
Event: telephone-event;rate=1000
Content-Type: audio/telephone-event
Content-Length: 4
0x0B0F0300
```

Exceptions and Limitations

The following limitations apply to the implementation of this feature on the Cisco BTS 10200 Softswitch:

- The system does not support out-of-band (OOB) DTMF relay for local SIP subscribers (subscribers registered directly with the Cisco BTS 10200 Softswitch).
- The system does not support inbound DTMF messages, and responds as follows when it receives an inbound DTMF message:
  - If the system receives an incoming NOTIFY for an event name other than “message_summary” (voice mail notification), it rejects the NOTIFY with a 400 (Unknown Event Specified) response.
  - If the system receives an incoming INFO with any content on a SIP trunk, it rejects the message with a 501 (Not Implemented) response.
  - If the system receives an INFO with a DTMF attachment on a SIP-T trunk during a connected call, it rejects the message with a 415 (Unsupported media type) response. This is because the system accepts only ISUP attachments on a SIP-T trunk during a connected call, and rejects all other attachment types with a 415 response.
  - If the system receives an INFO or NOTIFY message out of dialog, it rejects the message with a 481 (Call Leg/Transaction does not exist) response.
  - If the system receives an INFO before a call is in connected state, or from a subscriber, it rejects the message with a 501 (Not Implemented) response.

Asserted Identity and User-Level Privacy

The Asserted Identity feature is described in RFC 3325 and enables a network of trusted SIP servers to assert the identity of authenticated users. According to RFC 3323, when privacy features are applied to SIP messages, the calling party information (ANI) is unavailable to network elements in a trusted network domain, and inhibits network features such as call trace. The asserted identity allows these features to work because the ANI is provided in an asserted identity header, and shared across all network nodes in the trust domain. When the SIP message is exiting a trust domain, the header may be removed for privacy requirements.

Asserted identity is limited in its usage to specialized networks with trust domains as specified in RFC 3325. In Cisco BTS 10200, it is provided only in a limited context. This feature is associated to a Cisco BTS 10200 SIP trunk. It is designed to map calling party information from SS7 (or other non-SIP networks) into a SIP network as defined by the PacketCable CMSS 1.5 specification.

The feature is enabled by setting the USE-PAI-HDR-FOR-ANI flag in the SIP trunk group profile. If this flag is set to Y, calling party information is derived exclusively from the PAI header on inbound calls. For outbound calls, a PAI header is always sent with the calling party information if provided. If this flag is set to N, calling party information is mapped, sent, and received using the From: header. Details of

mapping ANI using the SIP From: header on Cisco BTS 10200 can be obtained from your Cisco account team. A provisioning example is provided in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

The SIP asserted identity header provides the calling name and number values. Cisco BTS 10200 support for the privacy specification RFC 3323 is limited to the use of the privacy header with value of `id' to indicate the calling number presentation indication when this feature is enabled. The presence of the SIP privacy header in the message with a value of `id' indicates the calling number is restricted; otherwise, it is not restricted.

Note A separate flag in the Cisco BTS 10200 SIP trunk group profile provides user-level privacy to the outbound SIP INVITE message. This is separate from the Asserted Identity feature. The privacy feature is enabled by setting the APPLY-USER-PRIVACY flag. If set to Y, if the originator requested privacy, aspects of the calling party information in the initial outbound SIP INVITE are hidden. These aspects include calling name and number in the From: header and Contact header. Privacy is only applied when either the calling party name or number have presentation restrictions and this flag is active. If set to N, user-level privacy is not applied.

The Cisco BTS 10200 does not evaluate the trusted network domain for calls in and out of the Cisco BTS 10200. The asserted identity header is honored if it is received on a SIP trunk, and sent if the feature is enabled, (providing ANI information is available). Therefore, this feature assumes that everything is trusted incoming and outgoing.

Note Do not rely on asserted identity to provide a trusted ANI if the Cisco BTS 10200 receives an ANI from non-trusted call sources.

An example of ANI information provided by the Asserted Identity and Privacy headers is shown below. In this case, the display name is ‘Jim’ and the number is 4692551234. The number presentation is restricted:

```
P-Asserted-Identity: "Jim" <sip:+14692551234@cisco.com>
Privacy: id
```

If the privacy header did not exist, it would reflect that the calling number presentation is allowed.

Third-Party Call Control

The role of a third-party call control (3PCC) controller is to initiate a call first to one endpoint, then to the other endpoint, and connect the two endpoints together in a two-party call. This allows for applications like operator placed calls, and call features like ‘click-to-dial’ where a user clicks a link on a Web browser to place a call.

Note Support for the 3PCC feature on Cisco BTS 10200 only deals with calls sent and received from a 3PCC controller, not Cisco BTS 10200 as a controller itself.

SIP call type of 3PCC have a property that the initial SIP Invite message sent does not include an SDP attachment. Cisco BTS 10200 requires offering SDP in the 200 response to INVITE, and answering SDP in the ACK. Feature support is limited to this message sequence. If SDP is received in 180 class response, it is ignored, regardless if the response is reliable or not.

Note H.323 slow start originating calls to SIP also result in an initial INVITE without SDP.

The Cisco BTS 10200 SIP trunk detects this message sequence and handles it dynamically. No provisioning is required.

ANI-Based Routing

ANI-based routing is used when incoming calls on a Cisco BTS 10200 SIP trunk require routing decisions based on more than simply the properties of the trunk the call was received. In this case, more information is required, including the properties of the originating business group which is not local to this Cisco BTS 10200. This information is required when the business groups are managed by another switch communicating with Cisco BTS 10200 using a single SIP trunk, and each business group has carrier preferences managed by this Cisco BTS 10200.

In Cisco BTS 10200, a subscriber is provisioned to represent each business group. Each of the subscribers is associated, by provisioning, to the SIP trunk toward the remote switch managing these groups. Each subscriber associated to the SIP trunk is assigned a range of numbers and properties specific to a business group. When a call is received on the SIP trunk, the called party number from the SIP INVITE message is used to select a subscriber associated to the trunk based on the subscriber's range of numbers. The selected subscriber provides the properties of the business group for routing.

Trunk Group Audit for the SIP Adapter

The Trunk Group audit mechanism verifies a trunk's operational status on a periodic basis. The mechanism is also triggered if communication problems are detected on the trunk.

The feature is enabled on a trunk-group using the STATUS-MONITORING flag. The number of failures needed to classify a trunk as out of service (OOS) is configured by means of the AUDIT-THRESHOLD on the softsw-tg-profile table, and the quiet interval before an audit is launched on a trunk is controlled by the TRUNK-AUDIT-INTERVAL in the CA-CONFIG table.

When not explicitly configured, the default values are as follows:

- STATUS-MONITORING flag (N)
- AUDIT-THRESHOLD (3)
- TRUNK-AUDIT-INTERVAL (3 minutes)

The Trunk Group audit mechanism utilizes the SIP protocol. The SIP OPTIONS method, with the Max_Forwards header value of 1, detects if a trunk is responsive. The response the audit OPTIONS receives may be an error message, but as long as a response is received, the trunk is deemed operationally in service (oper-INS).

A trunk is deemed operationally in service when any of the following occurs:

1. An initial INVITE message is received on the trunk.
2. A final response is received for a session initiating SIP message sent on the trunk. Currently, this is a SIP INVITE.
3. A final response is received for a SIP OPTIONS message sent on the trunk.

The first occurrence, above, restricts messages to initial INVITEs because subsequent INVITEs may be sent directly to Cisco BTS 10200 from an end-point proxied by a trunk. In the second occurrence, unless the trunk end-point performs a Record-Route, responses to subsequent messages in a dialog are sent

directly from the remote user agent client (UAC), when the trunk is playing a proxy role. If the trunk is playing the role of a back-to-back user agent, every response is indicative of the trunk liveness (INS). Since the role of the trunk is unknown, the restriction above is applied.

A trunk is marked operationally out of service (oper-OOS) when any of the following occurs:

1. An OPTIONS message sent for the purpose of audit times out and the trunk is not SRV.

In this case, the OPTIONS message was transmitted 11 times, to the hosts that the trunk's TSAP resolved to, in 32 seconds. Most likely, there are few hosts and the message was transmitted more than once to each host, which is enough to deem the trunk out of service.

SRV trunks are excluded from this because SRV potentially translates to more than 11 hosts, so a single OPTIONS message is not sufficient for deeming the trunk out of service.

2. A communication failure increments the count of such failures over a provisioned AUDIT-THRESHOLD in the Softswitch Trunk Group Profile.

Possible communication failures include:

- A transport-level send failure (over UDP or TCP) for an initial INVITE, CANCEL of an initial INVITE, ACK of a failure response to an initial INVITE or an OPTIONS sent to audit the trunk. This includes DNS resolution failures.
- A timeout on an initial INVITE, CANCEL of an initial INVITE or OPTIONS.
- A No-ACK timeout for a failure response to an initial INVITE.

If a Trunk Group is provisioned with STATUS-MONITORING = Y, and is administratively in service, audits occur in the following conditions.

- A communication error was reported on the trunk; for example, a request to a trunk times out, or a final error response to an INVITE sent on the trunk times out.
- A trunk is marked out of service. This results in a periodic audit of AUDIT_TIMER_INTERVAL. This parameter is specified in the CA_CONFIG table, with a default value of two seconds.
- No communication has occurred on the trunk for the provisioned AUDIT-INTERVAL in the Softswitch Trunk Group Profile. This is a periodic audit.

Note A SIP trunk's operational state is maintained in the trunk-group record, and is based on communication between Cisco BTS 10200 Softswitch and the trunk. The trunk is monitored only when status-monitoring is enabled, through provisioning, on the trunk-group record, and if the trunk is administratively in service.

When status-monitoring is turned on and the trunk is administratively in service, Cisco BTS 10200 sends an OPTIONS message periodically on the trunk if it is operationally out of service, or has had a long quiet period. When status-monitoring is turned off, an operationally out of service trunk is brought back into service only by receiving a message on the trunk, or by using the command line interface (CLI) Control command to first put it administratively out of service, and then put it back administratively in service.

SIP Route Advance

Using SIP trunk audit triggers another Cisco BTS 10200 feature, route advance.

When a SIP trunk has been detected and marked operational OOS by the SIP trunk audit, a route advance is automatically performed by Cisco BTS 10200, if there are additional routes provisioned to the called party.

Prior to implementing SIP trunk audit, the trunks were marked oper-INS, so Route Advance did not occur.

Cisco BTS 10200 has previously utilized the route advance feature for non-SIP trunks, and it is now enabled for SIP trunks as well.

Audit Occurrence

A Trunk Group with STATUS-MONITORING = Y provisioned, and which is ADMIN-INS, is audited under one of the following conditions.

1. A communication error has been reported on the trunk; for example, a request to a trunk times out, or a final error response to an INVITE sent on the trunk times out.
2. A trunk is marked OOS. This is really not a separate condition, and is subsumed by the previous condition.
3. No communication has occurred on the trunk for the provisioned TRUNK-AUDIT-INTERVAL in the CA-CONFIG. This is a periodic audit.

Modified Tables and Fields

Changes were made to the following tables and fields.

TRUNK-GRP Table

The following field was added to the TRUNK_GRP table.

Table 3-1 TRUNK_GRP Table

Type	PK/FK	Type	Values	Mandatory/ Optional
STATUS-MONITORING Trunk Group Status Monitoring Indicator. Determines whether a trunk group should be monitored whenever call failures resulting from timeouts occur. If set to 'Y,' and trunk-grp type is SIP or SIPT, an OPTIONS request is sent over this trunk periodically, to determine its status.		CHAR(1)	Y/N (Default=N	O

SOFTSW_TG_PROFILE Table

The following field was added to the SOFTSW_TG_PROFILE table.

Table 3-2 SOFTSW_TG_PROFILE Table

Type	PK/FK	Type	Values	Mandatory/ Optional
AUDIT-THRESHOLD Number of consecutive communication timeouts (SIP transaction timeouts) that will trigger a trunk group with this profile to be put out of service.		INTEGER	RANGE (1-10) DEFAULT=3	O

CA_CONFIG Table

The following entry was added to the CA_CONFIG table.

Table 3-3 CA_CONFIG Table

Type	PK/FK	Type	Values	Mandatory/ Optional
TRUNK-AUDIT-INTERVAL Interval in minutes for auditing SIP trunks. An OPTIONS request will be sent to an oper-INS trunk, during periods of inactivity, each time this interval is reached.		INTEGER	RANGE (1-10) DEFAULT=3	O

Alarms

The new SIGNALLING (142) alarm, SIP Softswitch Trunk Out Of Service, is defined for this feature. The alarm is issued for one of two reasons:

1. The Cisco BTS 10200 is unable to communicate with a remote SIP party (Call-Agent or Proxy) over a SIP or SIP-T trunk.
2. A remote SIP party is not operational.

When the alarm is issued for the first reason, Cisco BTS 10200 verifies that the DNS resolution exists, if the TSAP address of the remote entity is a domain name. Then, Cisco BTS 10200 verifies that the remote entity is reachable by ICMP ping, using the Trunk TSAP address from the Event Report.

If the same alarm is reported on all the Softswitch trunk groups, Cisco BTS 10200 verifies that the network connection is operational.

If the remote SIP party is not operational, and the ping is not successful, Cisco BTS 10200 diagnoses the issue that prevents the TSAP address from being reached. It then verifies that the SIP application is running on the remote host, and listening on the port specified in the TSAP address.

OPTIONS Message

The following example shows a SIP OPTIONS message sent out to audit the liveness of a SIP trunk.

```
OPTIONS sip: vmserver.globalsys.net:11617 SIP/2.0
Via: SIP/2.0/UDP prica20:15000;branch=z9hG4bK_av617_7801
From: <sip:prica20>;tag=1_av617_f11_3429
To: <sip:vmserver.globalsys.net>
Call-ID: 1726021128@prica20
CSeq: 1 OPTIONS
Max-Forwards: 1
Supported: 100rel,precondition,timer
Contact: <sip:prica20:15000>
Content-Length: 0
```

T.38 Fax Relay Call Agent Controlled Mode Across SIP Trunk Interface

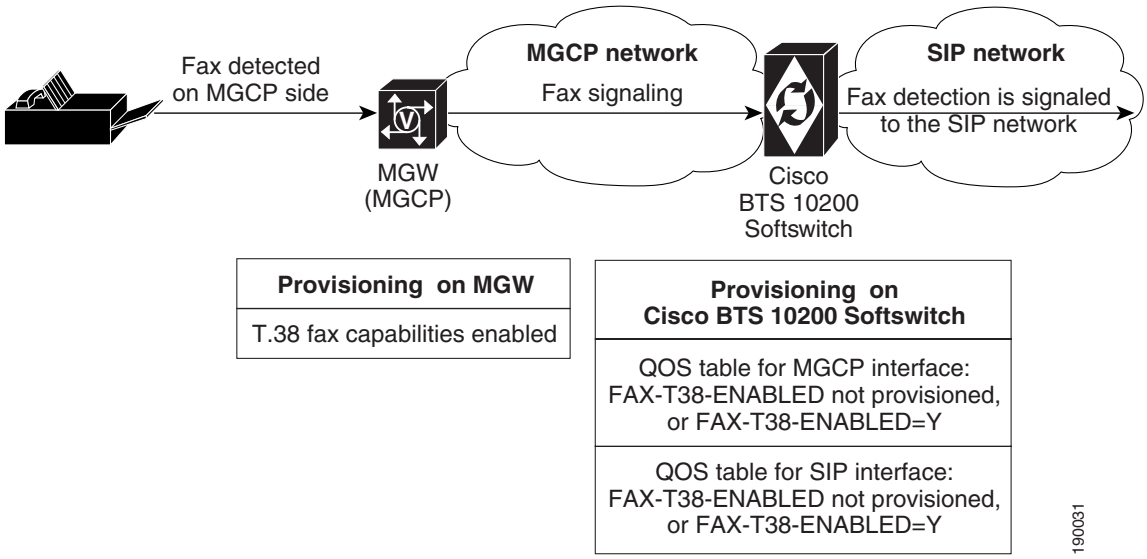
The Cisco BTS 10200 Softswitch supports T.38 fax interworking among devices that use MGCP, SIP, and H.323 protocols. There are several provisionable tokens in the Cisco BTS 10200 Softswitch database (in the MGW-PROFILE, QOS, H323-TG-PROFILE, H323-TERM-PROFILE, and CA-CONFIG tables) that affect the T.38 fax treatment on MGCP and H.323 interfaces. However, the Cisco BTS 10200 Softswitch SIP interface always allows switching to T.38 fax when an incoming fax is detected from the SIP network, regardless of the presence or absence of this provisioning.

For an MGCP to SIP call on the Cisco BTS 10200 Softswitch, if QoS is provisioned on the Cisco BTS 10200 Softswitch SIP interface with the FAX-T38-ENABLED field set to N, then the T.38 fax feature is disabled on the MGCP interface. The MGCP interface does not initiate T.38 procedures on fax detection, but it supports fax detection from the SIP network. The SIP interface is not affected by this provisioned value; it always supports T.38 procedures in any direction.

When the Cisco BTS 10200 Softswitch SIP interface sends T.38 capability attributes out the SIP network, it uses the standard format of RFC3407.

Figure 3-3 shows an example of MGCP and SIP interworking.

Figure 3-3 Example of MGCP and SIP Interworking for T.38 Fax



For additional information about T.38 fax features on the Cisco BTS 10200 Softswitch, see the following documents:

- The T.38 fax relay section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document.
- The T.38 fax relay provisioning section in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Voice-Mail Support

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

The Cisco BTS 10200 Softswitch supports a SIP trunk interface to external voice-mail (VM) application servers. It also supports defining voice mail as a subscriber extension within a Centrex group.

This chapter contains the following sections:

Note For SIP-specific VM provisioning details, see the "Provisioning Voice Mail" section in the *Cisco BTS 10200 Softswitch SIP PRotocol Provisioning Guide*. For general VM provisioning details, see the VM provisioning section in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

General Feature Description

With this feature, the Cisco BTS 10200 SIP interface can receive notification from a voice mail (VM) server. The notification indicates the message waiting status of a Cisco BTS 10200 local subscriber, and allows Cisco BTS 10200 to provide message waiting indication (MWI) on the subscriber's handset. The notification indicates the message waiting status of a Cisco BTS 10200 local subscriber, and allows Cisco BTS 10200 to provide message waiting indication (MWI) on the subscriber's handset.

SIP trunks interconnecting the Cisco BTS 10200 Softswitch to an external VM server must be provisioned as SIP VM trunks by setting the VM flag (voice-mail-trunk-grp) for these trunks in the softsw-tg-profile table. (See the softsw-tg-profile table in the *Cisco BTS 10200 Softswitch Command Line Reference Guide*.)

Voice-Mail Actions

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

- Calling Back a Message Depositor

Voice-Mail Deposit

There are two methods to deposit voice mail. In the first, the subscriber dials the pilot number for the voice-mail (VM) server and the call terminates on the voice-mail trunk. The voice-mail 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 Cisco 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 Cisco BTS 10200, such as CFNA, CFU, CFB, and specifies the forwarding number as the pilot number of the voice-mail server.

Message Waiting Indicator Notification

When a voice mail is deposited for a subscriber, the voice-mail server sends a notification to Cisco BTS 10200. In case the subscriber is on a SIP phone, Cisco BTS 10200 sends a SIP NOTIFY message to the phone to turn on the SIP phone Message Waiting Indicator (MWI). The number in the Notify message Request URL (which is the assigned subscriber number) identifies the subscriber.

Note For MGCP subscribers, Cisco 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 may be visual (a lamp, an envelope or other icon on a display) or may be aural, such as a stutter dial tone when the user next goes off-hook.

Cisco BTS 10200 implements the draft-ietf-sipping-MWI-01.txt with the following caveat: Cisco BTS 10200 supports receiving unsolicited NOTIFYs from a voice-mail system; however, it does not support subscribing to these notifications. Further, Cisco 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 this notification.

Retrieving Voice Mail

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

Once the voice mail is retrieved, the voice-mail server sends a Notify message to Cisco BTS 10200 to turn off the MWI indicator.

Calling Back a Message Depositor

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

Voice-Mail Implementation for Centrex Subscribers

A voice-mail (VM) application server may provide VM service for Cisco BTS 10200 Centrex subscribers from multiple Centrex groups. For the VM server to identify the subscriber and provide service configured for a Centrex group, it requires Cisco BTS 10200 to indicate the Centrex group with which the subscriber is associated.

When Cisco 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 messages waiting for a Cisco BTS 10200 Centrex subscriber, it must identify the Centrex group in the request URI of the NOTIFY message sent to the Cisco BTS 10200.

For any INVITE sent out a SIP trunk by Cisco BTS 10200 to the VM server, a Cisco BTS 10200 proprietary SIP URL parameter ‘bgid’ is added to the ‘From:’, ‘To:’, ‘Diversion:’ and Request URIs, if the user part of those URLs contain 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 Cisco BTS 10200 of a message waiting indication for a Centrex subscriber, the VM server sends a Notify SIP request to the Cisco BTS 10200 with a Centrex number format in the Request URL, and an associated ‘bgid’ parameter identifying the Centrex group associated to the subscriber. When the VM server initiates a call to a Cisco 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 to the subscriber.

The BGID parameter in the ReqUri of a INVITE originated from the voice-mail 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 Cisco BTS 10200 identifies the subscriber in the targeted Centrex group, whose MWI lamp will turn on or off.

Cisco BTS 10200 does not support calls between Centrex groups using extension dialing. Therefore, the ‘bgid’ parameter has an identical value if 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 to specify the ‘bgid’ parameter value. One trunk is provisioned for each Centrex group having a ‘bgid’ value of the associated 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.

For calls received on these 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. For general VM provisioning details, see "Provisioning Voice Mail" in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

Database Tables

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

This chapter addresses only the changed or new database tables used for Cisco BTS 10200 Release 4.5 SIP support. The chapter does not include information on any other Cisco BTS 10200 tables.

For information on how to provision the SIP devices, or how to map the configuration parameters to the Cisco BTS 10200 provisioning tables, refer to the Cisco BTS 10200 Softswitch Phone Mapping in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

The following tables were updated for Release 4.5:

- Softswitch Trunk Group Profile
- Trunk Group
- Subscriber
- Trigger ID
- Activity and Activity-Base

Additionally, there are new tables in Release 4.5, including:

- Address of Record to Subscriber
- Authentication Realm
- MAC to Subscriber
- Serving Domain Name
- User Authentication
- SIP Timer Profile
- SIP Adaptor Configuration Parameters (CA-CONFIG)

For more information on the changed or new tables, refer to the *Cisco BTS 10200 CLI Guide*. Also refer to the Cisco BTS 10200 Softswitch Phone Mapping section of the *Cisco BTS 10200 SIP Protocol Provisioning Guide*.

Changed Tables

The following two tables were in use by prior releases of Cisco BTS 10200 Softswitch. However, changes were made to the tables.

Softswitch Trunk Group Profile

The Softswitch Trunk Group Profile (SOFTSW-TG-PROFILE) table holds all the information specific to a Softswitch trunk, such as ID, protocol, indicators and echo suppression. Multiple softswitch trunk groups can share the softsw-tg-profile record. An ID must be created in this table before adding entries for SIP trunks to the Trunk Group table.

The following fields were modified for the SOFTSW-TG-PROFILE table:

- SIPT-ISUP-VER
- VOICE-MAIL-TRUNK-GRP
- TRUNK-SUB-GRP-TYPE

Several tokens are obsolete as of Release 4.5.x. See the details in Table 1 below.

Rules

- If PROTOCOL-TYPE=SIP-T, then SIPT-ISUP-VER must be specified. (Release 4.5)
- The SIPT-ISUP-VER token must be defined in the SIPT ISUP Version Base table. (Release 4.5)

Table 1 SOFTSW-TG-PROFILE Table Requirements

Table Name	SOFTSW-TG-PROFILE
Table Containment Area	Call Agent, EMS
Command Line Actions	Show, add, change, and delete

`show softsw-tg-profile id=softprf1;`
`add softsw-tg-profile id=softprf1; protocol-type=sip-t;`
`change softsw-tg-profile id=softprf1; send-cpn=n;`
`delete softsw-tg-profile id=softprf1;`	

Primary Key Token(s)	ID
Add Rules	See Rules, above
Change Rules	None
Delete Rules	ID cannot exist in any TRUNK-GRP::TG-PROFILE-ID where TG-TYPE=SOFTSW.

Table 2 SOFTSW-TG-PROFILE Syntax Description

ID	Primary Key. Unique ID for this trunk group profile. VARCHAR(16): 1 – 16 ASCII characters.
PROTOCOL-TYPE	Specifies the type of signaling for this trunk group. It controls the message type sent between two Cisco BTS 10200 Softswitches. For example, if the protocol-type is SIP-T, then the Cisco BTS 10200 Softswitch sends a SIP-T message, which is a normal SIP ASCII message plus an ISUP MIME attachment. In this case, the origination type can be ISDN, SS7, CAS, MGCP, and so forth. The origination type does not matter. However, if the protocol-type is SIP, then the Cisco BTS 10200 Softswitch sends only an ASCII SIP message without an ISUP MIME attachment. VARCHAR(9): 1–9 ASCII characters. Permitted values are: SIP Signaling via SIP. [1] multimedia sessions across the Internet. SIP_T Signaling using SIP-T protocol. SIP-T is an inter Call Agent protocol; SIP-GTD protocol is a normalized inter Call Agent protocol. CMSS Not supported. CMSS stands for Call Management System Signaling. It is the protocol used for communication between PacketCable Cable (CMS) switches when a call spans across them (similar to Cisco BTS 10200 calls to Cisco BTS 10200 over SIP). CMSS trunk types are used exclusively for CMS switches.
APPLY-USER-PRIVACY (Release 4.5)	Specifies whether to apply user privacy. CHAR(1): Y/N (Default = N). Y—If the originator requested privacy, aspects of the calling party information (such as the calling name and number in the From:header) in the initial outbound SIP INVITE is hidden. Privacy is requested when either the calling party name or number have presentation restrictions. N—User level privacy is not applied.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DESCRIPTION (EMS-only field)	Described by the service provider. VARCHAR(64): 1–64 ASCII characters.

DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
DIVERSION-HEADER-SUPP	Indicates if SIP Diversion Header is supported or not. This header conveys diversion information from other SIP user agents and proxies to the called user agent. This information can be used for enhanced features, including Unified Messaging, Third-Party voice mail, and Automatic Call Distribution (ACD). The most common use of the Diversion Header in the Cisco BTS 10200 Softswitch is for call forwarding features. Both tokens can be no (N) but only one can be yes (Y). Not applicable to Release 4.5. CHAR(1): Y/N (Default = N).
DNS-SRV-ADV-ON-RETRANS-TIMEOUT (Release 4.5)	Controls whether the Cisco BTS 10200 Softswitch advances to the next server entry associated with the server (SVR) TSAP address on the trunk, for subsequent retransmission, when a timeout occurs. **Note** This token applies if dns-srv-supp = dns-srv-supp-rfc2782-labels. It does not apply to non-SRV trunks. CHAR(1): Y/N (Default = Y). N—RFC3263 compliant behavior prevails. All retransmissions go to the same server within the list associated with an SRV record. Y—Existing Cisco BTS 10200 Softswitch behavior prevails. Each retransmission goes to a different server in the list associated with the SRV record.
DNS-SRV-SUPP	DNS service (SRV) resolution needed flag. VARCHAR(16): 1–16 ASCII characters. Permitted values are: NONE (Default) RFC2782-LABELS—Prepend the protocol and service labels with an underscore.

DTMF-RELAY-METHOD	Specifies which way to send an out-of-band DTMF Relay. VARCHAR(8): 1–8 ASCII characters. Permitted values are: NONE (DEFAULT) Unsolicited DTMF Relay – Not supported. NOTIFY DTMF Relay supported based on Subscribe / Notify Method. INFO DTMF Relay supported based on INFO Method.
ECHO-SUPP-REQUIRED (Obsolete as of Release 4.5)	Echo Suppression Required indicator. CHAR(1) Y/N (Default = N)
ES-SUPP (Release 4.4.1)	Specifies whether to send CALEA information on a SIP CMSS interface. Used only for a CMSS type trunk group. Set to Y in case the equipment on the other side of a CMSS SIP interface supports CALEA requirements. CHAR(1): Y/N (Default = N). N— Disable sending of CALEA information on SIP CMSS interface. Y— Enable sending of CALEA information on SIP CMSS interface.
ES-SUPP (Release 4.5)	Used for CALEA. When this token is enabled, surveillance information as defined in Section 8 of RFC 3603 is sent when surveillance is required on the call, and surveillance cannot be performed on this switch. This requires the remote SIP entity interfacing the SIP trunk to support surveillance procedures. CHAR(1): Y/N (Default = N). N— Disable sending of CALEA information on SIP interface. Y— Enable sending of CALEA information on SIP interface.
GTD-MODE (Release 4.5)	Specifies whether to use the compact (default) or verbose mode to encode messages for the SIP-T/GTD trunk group. VARCHAR(8): 1–8 ASCII characters. Permitted values are: COMPACT (Default) VERBOSE

HOP-COUNTER-MAX (Release 4.5)	Applies only to received SIP Invite messages contain a max-forwards value in which down to build the hop counter. If the hop max-forwards is greater than this value, value acts as a ceiling for the derived hop. INTEGER: 10–20 (Default = 20).
HOP-COUNTER-SUPP (Release 4.5)	Used for received SIP Invite messages that are not SIP-T and contain a max-forwards value. The default sets the hop counter based on the received max-forwards value. If this flag is set to N, the hop counter field is not populated using the max-forwards value. CHAR(1): Y/N (Default = Y).
INBAND-TONE-AVAILABLE	Send release or provide tone/announcement. CHAR(1)Y/N (Default = Y)
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
MAX-FORWARDS (Release 4.5)	Specifies when an outbound SIP Invite message requires an initial maximum forwards value. INTEGER: 4–80 (Default = 70).
NON-SRV-TRANSPORT **Note** This parameter will only have meaning when DNS-SRV-SUPP is set to NONE.	Specifies the transport mechanism to use for signaling. This token is used only when dns-srv-supp=none. VARCHAR(8): 1–8 ASCII characters. Permitted values are: UDP (Default)— Use UDP unless message size requires TCP as described in RFC 3261 and RFC 3263. TCP— Use TCP. UDP-ONLY— Use UDP. Does not attempt TCP even if message size exceeds limits described in RFC 3261 and RFC 3263.

ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
PRACK-FLAG	Specifies if an Invite messages sent on this trunk group require reliable provisional responses. If yes, provisional responses like alerting are delivered. Used with SIP-T. CHAR(1): Y/N (Default = N).
REDIRECT-SUPPORTED	Specifies if the Cisco BTS 10200 Softswitch honors a 3xx class, such as a redirection response for an Invite message sent by the Cisco BTS 10200 Softswitch. VARCHAR(32): 1–32 ASCII characters. Permitted values are: VALID-DOMAINS-ONLY (Default)— If the host name field in the SIP URI of a 3XX contact used for call redirection does not represent this Cisco BTS 10200 Softswitch or a Cisco BTS 10200 Softswitch SIP trunk, then the call is redirected using the SIP trunk used on the previous call redirection. If there was not a previous call redirection, then the SIP trunk that sent the initial Invite is used. If the profile of the selected SIP trunk restricts redirection to only valid domains, then this redirection is blocked and the next contact is tried. Otherwise, it is redirected and the contact URI is used as the request URI of the redirected call. ALL-DOMAINS— Redirects to any allowed domain. NONE— No redirects allowed.
REFER-ALLOWED	Call Transfer allowed on an SS trunk. CHAR(1): Y / N (Default = N).
SATELLITE-CIRCUIT **(Obsolete as of Release 4.5)**	CHAR(1)Y/N (Default = N)
SCALE-FACTOR (Release 4.5)	Used for conversions between hop counter and max-forwards values; allows no-conversion, one-half, one-third, and one-quarter conversion factors. The default provides a scale relative to the maximum values: if the hop counter is 20, a scale factor of 4 converts to a max-forwards value of 80. Using the default means no conversion. INTEGER: 1–4 (Default = 1).
SEND-ATP **(Obsolete in Release 4.5)**	Send Access Transport Parameter indicator. CHAR(1)Y/N (Default = Y)

SEND-CIC-PARAM (Release 4.5)	Specifies whether the CIC parameter is included in the request URL for outbound SIP calls. CHAR(1): Y/N (Default = Y)
SEND-CPN **(Obsolete in Release 4.5)**	Send Calling Party Number indicator. CHAR(1)Y/N (Default = Y)
SEND-FULL-E164 (Release 4.5)	When enabled, all SIP phone numbers contained in SIP messages sent from the Cisco BTS 10200 Softswitch that have an NOA of national significance are represented as fully qualified E.164 numbers prefixed with the local country code and plus sign. This conforms to IETF RFC 3398 Section 12.1. When disabled, national numbers are sent without a country code and plus sign prefix. Numbers of international significance are always sent with a plus sign and country code regardless of this flag setting. CHAR(1): Y/N (Default = N). **Note** The Home Country code is defined in the Call Agent Configuration table.
SEND-GAP **(Obsolete in Release 4.5)**	Send Generic Address Parameter indicator. CHAR(1)Y/N (Default = Y)
SEND-GN **(Obsolete in Release 4.5)**	Send Generic Name indicator. CHAR(1)Y/N (Default = Y)
SEND-JIP **(Obsolete in Release 4.5)**	Send Jurisdiction Information Parameter indicator. CHAR(1)Y/N (Default = Y)
SEND-GAP **(Obsolete in Release 4.5)**	CHAR(1)Y/N (Default = Y)
SEND-OCN **(Obsolete in Release 4.5)**	CHAR(1)Y/N (Default = Y)
SEND-REDIR-NUM **(Obsolete in Release 4.5)**	CHAR(1)Y/N (Default = Y)
SEND-SIP-181-RESP (Release 4.5.1)	Specifies whether the Cisco BTS 10200 Softswitch transmits a 181 response message to a UAC when the terminating side of the Cisco BTS 10200 Softswitch forwarded the call. CHAR(1): Y/N (Default = N)
SESSION-TIMER-ALLOWED	Specifies whether a session timer is allowed. CHAR(1)Y / N (DEFAULT=N)

SIP-SIG-LOWDELAY	Specifies whether to set low delay. Low delay refers to the waiting time, or latency involved in sending and receiving a packet. You can set various options on the TCP socket to tune or optimize for certain performance parameters. CHAR(1): Y/N (Default = Y). **Caution** Cisco does not recommend using any value other than the specified default. Changing this value from its default may significantly impact network performance. Contact Cisco TAC for further information. If you prefer to use DSCP values instead of TOS values, derive the appropriate TOS values using the DSCP/TOS mapping information in the CLI Guide, Appendix F, "Data Values for TOS, DSCP, and PHB Parameters."
SIP-SIG-PRECEDENCE	Specifies the designation assigned to a phone call by the caller to indicate the relative urgency (and thus the order of handling) of a call. It also sends an indication to the called party of the order in which the call is answered. VARCHAR(16): 1–16 ASCII characters. Permitted values are: FLASH (Default = 3) NETCONTROL (= 7) INTERNETCONTROL (= 6) CRITICAL (= 5) FLASHOVERRIDE (= 4) IMMEDIATE (= 2) PRIORITY (= 1) ROUTINE (= 0) **Caution** Cisco does not recommend using any value other than the specified default. Changing this value from its default may significantly impact network performance. Contact Cisco TAC for further information. **Note** If you prefer to use DSCP values instead of TOS values, derive the appropriate TOS values using the DSCP/TOS mapping information in Appendix F, "Data Values for TOS, DSCP, and PHB Parameters."

SIP-SIG-RELIABILITY	Specifies whether to set reliability. Reliability refers to the dependability of packet delivery. CHAR(1): Y/N (Default = N). **Note** Cisco does not recommend using any value other than the specified default. Changing this value from its default may significantly impact network performance. Contact Cisco TAC for further information. **Note** If you prefer to use DSCP values instead of TOS values, derive the appropriate TOS values using the DSCP/TOS mapping information in the CLI Guide, Appendix F, "Data Values for TOS, DSCP, and PHB Parameters."
SIP-SIG-THROUGHPUT	Specifies whether to set throughput. Throughput refers to the actual amount of useful and nonredundant information that is transmitted or processed. The relationship between what went in one end of the network and what came out the other is a measure of the efficiency of that communications network. Throughput is a function of bandwidth, error performance, congestion, and other factors. CHAR(1): Y/N (Default = N). **Caution** Cisco does not recommend using any value other than the specified default. Changing this value from its default may significantly impact network performance. Contact Cisco TAC for further information. **Note** If you prefer to use DSCP values instead of TOS values, derive the appropriate TOS values using the DSCP/TOS mapping information in the CLI Guide, Appendix F, "Data Values for TOS, DSCP, and PHB Parameters."
SIP-TIMER-PROFILE-ID (Release 4.5)	Foreign key: Softswitch Trunk Group Profile table. Specifies the Timer Profile ID for the Softswitch Trunk Group Profile. VARCHAR(16): 1–16 ASCII characters.

SIPT-ISUP-VER	Mandatory if protocol-type=SIP-T. Defines the SIP-T or SIP-GTD version. Used only if protocol-type=SIP-T. Defined in the SIPT ISUP Version Base table. If the value defined in the SIPT ISUP Version Base table has a base value of sip-gtd, then the version is a SIP-GTD type. Otherwise, the version is a SIP-T type. VARCHAR(32): 1–32 ASCII characters. Permitted value is: GR317. **Note** Values other than GR317 are permitted as of Release 4.4.1.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).
TRUNK-SUB-GRP-TYPE	Specifies the parameter to be populated when trunk-sub-grp is defined in the Trunk Group table. VARCHAR(16): 1–16 ASCII characters. Permitted values are: NONE (Default)— Trunk-sub-grp is not used. BGID— Encode trunk-sub-grp in the BGID field of SIP-URI. BGID is a numeric field.
USE-PAI-HDR-FOR-ANI (Release 4.5)	Controls the p-asserted-id (PAI) header used to send and receive calling party information. **Note** When this token is set to Y, the calling party information is derived from the PAID header on inbound calls. If a SIP INVITE arrives at the Cisco BTS 10200 Softswitch without a PAID header, the Cisco BTS 10200 Softswitch treats the call as though it does not have calling party number. Features that rely on the calling number, such as Customer Originated Trace (COT, *57), may not work properly with use-pai-hdr-for-ani=Y if the incoming SIP INVITE does not have the PAID header. CHAR(1): Y/N (Default = N). Y— Calling party information is derived exclusively from the PAI header on inbound calls. For outbound calls, a PAI header is sent with the calling party information if provided. N— Calling party information is sent or received using the From:header.

VOICE-MAIL-TRUNK-GRP	Specifies whether the Softswitch trunk group is used for the voice-mail application. CHAR(1)Y/N (Default = N)
TRUNK-SUB-GRP-TYPE	VARCHAR(16): 1 – 16 ASCII characters NONE (Default) Trunk-Sub-Grp is not used. BGID Encode TRUNK-SUB-GRP in the BGID field of SIP-URI. BGID is a numeric field. TGID (Future) Encode TRUNK-SUB-GRP in the TGID field of SIP-URI

Trunk Group

The Trunk Group (trunk-grp) table identifies the trunk group and maps it to the associated media gateway. Table 3 indicates optional tokens that are required during provisioning based on the trunk group type.

The Cisco BTS 10200 Softswitch supports the following trunk group types: announcement, CAS, ISDN, SS7 and SOFTSW. The Trunk Group table defines common information based on the trunk group type. The Cisco BTS 10200 Softswitch supports announcement, CAS, ISDN, SS7 and SOFTSW trunk group profiles.

Table Name: TRUNK-GRP

Table Containment Area: Call Agent

The following fields were modified for the Trunk Group table:

- MGCP-PKG-TYPE
- SOFTSW-TSAP-ADDR
- TRUNK-SUB-GRP
- TG-PROFILE-ID
- SEL-POLICY

For more information about the Trunk Group table, refer to Trunk Group section of the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

Modifications

- Add TRUNK-SUB-GRP token.
- Add MGCP-PKG-TYPE – move MGCP-PKG-TYPE from TG-PROFILE to the TRUNK-GROUP Table.

Rules

- If TG_TYPE=SOFTSW, the combination of SOFT-TSAP-ADDR and TRUNK-SUB-GRP must be unique.

- If TG_TYPE=SS7, MGCP_PKG_TYPE should be either T OR IT.
- TG_TYPE=CAS, MGCP_PKG_TYPE should be one of DT, MS, MT, MO, MD.
- TG_TYPE=ANNC, MGCP_PKG_TYPE should be either TCL_CISCO, ANNC_CABLE_LABS.
- TG_TYPE=ISDN, MGCP_PKG_TYPE should be T.
- ELSE TYPE = NA
- If CAS-TG-PROFILE->SIG-TYPE is MF_OSS, then MGCP-PKG-TYPE should be MO.
- CSCEB32199
- DIAL-PLAN-ID is not requiredIF TG-TYPE=ANNC OR
- MAIN-SUB-ID ? NULL OR,
- DIRECTION=OUT.

Table 3 SOFTSW-TG-PROFILE Table Requirements

Table Name	TRUNK-GRP
Table Containment Area	Call Agent
Command Line Actions	Show, add, change, and delete

`show trunk-grp id=101;`
`add trunk-grp id=101; call-agent-id=CA146; tg-type=ss7; dial-plan-id=tg-dp;`
`dpc=101-55-103; tg-profile-id=SS71;call-ctrl-route-id=ccr1;`
`change trunk-grp id=101; cost=200;`
`delete trunk-grp id=101;;`	

Primary Key Token(s)	ID
Add Rules	ID exists in the carrier table; ID exists in the subscriber table. DIAL-PLAN-ID is required except if tg-typ=ANNC or if main-sub-id is not equal to NULL.
Change Rules	Ensure that the ID exists in the Subscriber table if entered; ensure the id exists in the Media Gateway table if entered. The DPC field cannot be changed.
Delete Rules	ID cannot exist in any subscriber::term-id; ID cannot exist in any trunk::term-id. ID cannot exist in any mlhg-terminal::term-id. Trunk group status must be OOS.
Transit Network Selection (TNS) Rules	If a call is interLATA and going to an access tandem (AT), the TNS parameter is sent. This is also known as direct distance, or domestic, dialing (DDD). If a call in international, the TNS parameter is sent. If a carrier ID is not assigned to a trunk group, the TNS parameter is sent. If a carrier ID is assigned to a trunk group, the TNS parameter is not sent.

Trunk/CIC Selection Rules	• Ascending—Whenever a outgoing call is needed, the Cisco BTS 10200 Softswitch always selects the trunk with the lowest available CIC. For example: – 3 trunks, CICs 1, 2 and 3 – outgoing call A uses CIC 1 – outgoing call B uses CIC 2 (call A has not released) – call A releases CIC 1 • outgoing call-C uses CIC 1 again since it is now available. • Descending—the reverse of ascending. The highest available CIC is always selected. • Cyclic Ascending (CASC)—when processing outgoing calls, the Cisco BTS 10200 Softswitch loops through all the trunks based on the ascending CIC sequence. For example: – 3 trunks, CICs 1, 2 and 3 – outgoing call A uses CIC 1 – outgoing call B uses CIC 2 (call A has not released) – call A releases CIC 1 – outgoing call C uses CIC 3 even though CIC 1 is idle and available. • Cyclic Descending (CDSC)—when processing outgoing calls, the Cisco BTS 10200 Softswitch loops through all the trunks based on the descending CIC sequence. For example: – 3 trunks, CICs 1, 2 and 3 – outgoing call A uses CIC 3 – outgoing call B uses CIC 2 (call A has not released) – call A releases CIC 3 – outgoing call C uses CIC 1 even though CIC 3 is idle and available.

MGCP-PKG-TYPE/TG-TYPE Rules	If mgcp-pkg-type = DT | MS | MT | MO, then it is valid only for CAS tg-type. If mgcp-pkg-type = MO, then MF-OSS-TYPE in the Channel Associated Signaling Trunk Group Profile table is required. If mgcp-pkg-type = CISCO-TCL | ANNC-CABLE-LABS, then it is valid only for ANNC tg-type. Mgcp-pkg-type=line allowed only when tg-type=cas and the corresponding CAS Trunk Group Profile has sig-type=line. (Release 4.5) If mgcp-pkg-type=mt, then direction=IN. (Release 4.5) If mgcp-pkg-type=mo, then direction=OUT. (Release 4.5) If tg-type=ISDN; then glare=ALL. If tg-type=ISDN, the mgcp-pkg-type is T or IT. If tg-type=SS7, the mgcp-pkg-type is T or IT. If tg-type=CAS, the mgcp-pkg-type is one of DT, MS, MT, or MO. If tg-type=CAS; then glare=SLAVE. If tg-type=ANNC, the mgcp-pkg-type is either tcl-cisco or annc-cable-labs. If tg-type=SOFTSW | H323, the mgcp-pkg-type is NA. If sig-type in the cas-tg-profile=mf-oss, then the mgcp-pkg-type=MO.
MO and MT Rules	When configuring a trunk group, set the direction token to OUT when the MGCP-PKG-TYPE is MO. When configuring a trunk group, set the direction token to IN when the MGCP-PKG-TYPE is MT.

Table 4 TG Syntax Description

* ID	Primary key. Trunk group number. INTEGER: 1-99999999.
* CALL-AGENT-ID	Foreign key: Call Agent table. Call Agent ID. Same as ID in Call Agent table. VARCHAR(8): 8 ASCII characters. Format is CAnnn or cannn where nnn = 001–999. 3 characters are reserved for Not Used use.

* TG-TYPE	Trunk group type. VARCHAR(6): 1–6 ASCII characters. Permitted values are: ANNC—Announcement. SOFTSW—Softswitch trunk group. CAS—Channel associated signaling. ISDN—Integrated Services Digital Network. SS7—Signaling System 7. H323—H.323 trunk group.
ALT-ROUTE-ON-CONG	Specifies whether to use an alternate route when there is traffic congestion. CHAR(1): Y/N (Default = N). Y—SKIP N—BLOCK
ANI-BASED-ROUTING	Used when there are multiple subscribers homing on the same trunk group. The ANI is used to determine the subscriber ID associated with the call. CHAR(1): Y/N (Default = N). Y—Determine subscriber ID based on the ANI. N—Use normal routing.
ANI-DIGMAN-ID	Foreign key: Digman Profile table. ANI (calling party number) digit manipulation ID. VARCHAR(16): 1–16 ASCII characters.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
CALL-CTRL-ROUTE-ID	Mandatory if tg-type = SS7. Foreign key: Call Control Route table. The Call Control Route ID. VARCHAR(16): 1–16 ASCII characters. **Note** This token cannot be changed.
CARRIER-ID	Carrier ID if direct trunk group to a carrier. Used during incoming call processing. Same as carrier-id in Carrier table. CHAR(4): 4 numeric characters—leading zeros count.
CAUSE-CODE-MAP-ID	Foreign key: Cause Code Map table. The cause code map ID. VARCHAR(16): 1–16 ASCII characters.
CLLI	Common Language Location Identifier for the remote switch. CHAR(11): Eleven ASCII characters.

COST	Relative cost value; used if TG selection is based on least cost routing (LCR). SMALLINT: 0–999.
DEFAULT-CHG	Default charge number. VARCHAR(16): 1–16 numeric digits.
DEL-DIGITS	Specifies the number of digits to delete. SMALLINT: 0–14 numeric characters. (Default = 0).
DESCRIPTION (EMS-only field)	Described by the service provider. VARCHAR(64): 1–64 ASCII characters.
DIAL-PLAN-ID	Foreign key: Dial Plan table. Specifies which dial plan ID to use. For trunk groups with a Main subscriber ID (CAS, ISDN), the Call Agent uses the dial-plan-id assigned to the trunk group (if available), else it uses the dial-plan-id assigned to the subscriber profile. VARCHAR(16): 1–16 ASCII characters.
DIRECTION	Direction of the trunk group. Can be incoming only, outgoing only, or both incoming and outgoing. If bothway, the glare parameter is required. VARCHAR(4): 1–4 ASCII characters. Permitted values are: BOTH (Default)—Bothway trunk group (used for both incoming and outgoing calls). OUT—Used for outgoing calls only. IN—Used for incoming calls only.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
DNIS-DIGMAN-ID	Foreign key: Digman Profile table. DNIS (called party number) digit manipulation ID. VARCHAR(16): 1–16 ASCII characters.
DPC	Not provisionable. Mandatory if tg-type=SS7. Destination Point Code if SS7. The DPC is automatically provisioned from the call-ctrl-route-id. VARCHAR(16): 1–16 ASCII characters.

GLARE	Used in bothway trunks: Defines how to resolve a glare condition—a bothway (simultaneous) trunk seizure. For example, an incoming and an outgoing call on the same endpoint. For ISDN trunk groups, glare *must* be set to ALL. Setting glare to SLAVE can cause CIC/trunk instability. VARCHAR(5): 1–5 ASCII characters. Permitted values are: SLAVE (Default)—This trunk group yields any trunk in glare condition. ALL—This trunk group is master of all trunks. EVEN—This trunk group is master of even numbered trunks. ODD—This trunk group is master of odd numbered trunks. PC—Not used. Point code driven. The higher point code is the master. Is allowed only for an SS7 trunk group.
H323-GW-ID	Mandatory if tg-type=h323. Foreign key: H.323 Gateway table. Specifies the gateway ID for this trunk group. VARCHAR(16): 1–16 ASCII characters.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
MAIN-SUB-ID	Foreign key: Subscriber table. Used for PBX subscribers. VARCHAR(30): 1–30 ASCII characters.
MGCP-PKG-TYPE	Determines the MGCP Package type for the announcement server. VARCHAR(16): 1–16 ASCII characters. Permitted values are: NA—(Default) For SIP and H.323 trunk groups. ANNC-CABLE-LABS—Announcement signaling type based on the Cable Labs package. AUTO—Used for CAS signaling on a combined trunk group (not supported). DT—DTMF package. IT—ISUP trunk package. LINE—Line package used for Test Line Access. MD—MF FGD package (Release 4.5) (Not supported). MO—MF operator trunks. MS—MF package. MT—MF terminating package. TCL-CISCO (Default)—Announcement signaling type for the Cisco AS5350/AS5400. T—Trunk package.

NUM-OF-TRUNKS (System generated)	Not provisionable. EMS provisions this field when trunks are provisioned for this trunk group. SMALLINT: 1–9999.
OPER-STATUS	Operational status. VARCHAR(5). Permitted values are: NF (Default)—Nonfaulty. FA—Faulty. NF-RB—Nonfaulty remotely blocked. FA-RB—Faulty remotely blocked.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
PERFORM-LNP-QUERY (Release 4.5)	Specifies whether to perform an LNP query. This token applies only to incoming calls (for ITU local LNP, when the LNP Profile lnp-db-type is RN). CHAR(1): Y/N (Default = N). Y —Perform an LNP Query if required based on the LNP Profile table and the acq-lnp-query token in the Destination table. This applies to both LNP Types: ACQ and QOR. Set this token to Y when the remote switch is not LNP-capable. N—An LNP query is not required as originating switch is LNP-capable or LNP is not required.
PFX-DIGITS	Specifies what digits to prefix. Digits are prefixed after the specified number of digits are deleted. VARCHAR(10): 1–10 ASCII characters.
POP-ID	Foreign key: POP table. Defines the number of POPs in a Call Agent; used for incoming trunk groups. VARCHAR(16): 1–16 ASCII characters.
QOS-ID	Foreign key: QOS table. Specifies whether or not to use QOS index for codec selection. VARCHAR(16): 1–16 ASCII characters. **Caution** This token must be provisioned to match the qos-id for the trunk in the Quality of Service table. If two MGWs are involved in a call, there are additional QoS requirements applicable for the trunk groups on each MGW. See the hptime and lptime token descriptions in the Quality of Service table.

REGION	Region of the incoming trunk group. VARCHAR(16): 1–16 ASCII characters.
REMOTE-SWITCH-LRN	LRN of the previous switch used for billing. VARCHAR(10): 1–10 numeric digits, in the format NPA-NXX-XXXX. (Default = 0).

Subscriber

The Subscriber (SUBSCRIBER) table defines the characteristics of a subscriber or group of subscribers in a Call Agent. All termination numbers reached by a DN must be set up as a subscriber. Any termination that can originate in the primary Call Agent must be set up as a subscriber (Residential, PBX, Business, Centrex, and so on). All terminations to customers, such as MLH, Centrex, must be defined as well.

The following fields have been modified for the Subscriber table:

- TERM-TYPE
- TERM-ID
- MGW-ID
- TGN-ID (or TG)
- POLICY_ID
- AOR_ID
- MAC-ID (EMS ONLY)

For more information about the Subscriber table, refer to the *Cisco BTS 10200 Softswitch Release Command Line Interface Reference Guide*.

Modifications to the table

- Add new TERM-TYPE=SIP and NONE.
- Add AOR index to the Subscriber Table (case insensitive)
- Add MAC Address for IP Phone Devices (supported for SIP)

Note In Release 4.5, the user portion of the AOR-ID must match the DN1 value for the subscriber.

Add Subscriber

1. If MAC-ID is specified, add an entry in the MAC2SUB Table
2. Provision Subscriber Table
3. Add sub-id to the aor2sub Table (if AOR-ID is NOT NULL)
4. Add sub-id to the mac2sub table (if MAC-ID is NOT NULL)

Change Subscriber AOR

The following tokens can not be changed via change subscriber command:

- AOR-ID (instead use change SUBSCRIBER-AOR command)
- MAC-ID (instead use change SUBSCRIBER-MAC-ID command)
- TERM-ID, MGW-ID (instead use change SUBSCRIBER-TERMINATION command)
- TERM-TYPE
- DN1 (instead use change SUBSCRIBER-DN command)

Table 5 SUBSCRIBER Table Requirements

Table Name	SUBSCRIBER
Table Containment Area	Call Agent, EMS, POTS Feature Server
Command Line Actions	Show, add, change, and delete
show subscriber id=cisco-main-number; **add subscriber id=cisco main number; name=wilmerwabash; dn1=972-671-2000;** **sub-profile-id=richardson;** **change subscriber id=cisco-main-number; category=ctxg-individual;** **name=wilmerwabashjr; status=temp-disconnected; privacy=full;** **delete subscriber id=cisco-main-number;**	
Primary Key Token(s)	ID
Add Rules	• term-id, mgw-id are required if category=mlhg-pref-indiv | ctxg-individual | mlhg-individual | individual. • no term-id, mgw-id if category= pbx | ctxg-tg; term-id, mgw-id optional if category=mlhg | ctxg-mlhg | ctxg. • mlhg-pref-list-id is required if category=mlhg-pref-indiv. • mlhg-id is required and exists if category=mlhg | mlhg-pref-indiv | mlhg-individual | ctxg-mlhg; ctxg-id is required and exists if category=ctxg | ctxg-individual | ctxg-mlhg | ctxg-tg; tgn-id is required and exists if category=pbx | ctxg-tg. • During split-npa, if ani-update-status=completed, subscriber provisioning should not allow dn1, dn2, dn3 that are in the old-npanxx.

Change Rules	• term-id, mgw-id are required if category=mlhg-pref-indiv | ctxg-individual | mlhg-individual | individual no term-id, mgw-id if category=ctxg-tg | pbx term-id, mgw-id optional if category=mlhg | ctxg-mlhg | ctxg. • mlhg-id is required and exists if category=mlhg | mlhg-pref-indiv | mlhg-individual | ctxg-mlhg mlhg-pref-list-id is required if category=mlhg-pref-indiv. • ctxg-id is required and exists if category=ctxg | ctxg-individual | ctxg-mlhg | ctxg-tg tgn-id is required and exists if category=pbx | ctxg-tg. • During split-npa, if ani-update-status=completed, subscriber provisioning should not allow a dn1 that is in the old-npanxx.
Delete Rules	ID does not exist in any ctxg::main-sub-id if category=ctxg. ID does not exist in any mlhg::main-sub-id if category=mlhg. ID does not exist in any tgn-id::main-sub-id if category=pbx | ctxg-tg. ID does not exist in any subscriber-service-profile::sub-id. ID does not exist in any subscriber-feature-data::sub-id.

Note Modified fields are in bold type.

Table 6 SUBSCRIBER Syntax Description

ID	Primary key. VARCHAR(30): 1 - 30 ASCII characters.
CATEGORY	VARCHAR(15). INDIVIDUAL (Default) Individual Subscriber. MLHG Main subscriber ID of a MLHG. MLHG-INDIVIDUAL Individual Subscriber within a MLHG. MLHG-PREF-INDIV Main subscriber ID of a preferential hunt list. CTXG Assigned to the main subscriber ID of a Centrex Group. CTXG-INDIVIDUAL Assigned to a Centrex Subscriber. CTXG-MLHG Assigned to a Centrex MLHG (e.g., attendant). CTXG-TG Assigned to Centrex Trunk Group. PBX Assigned to the main subscriber ID of a PBX. RACF Access DN for remote activation of Call Forwarding IVR Access DN for IVR.
NAME	VARCHAR(16): 1 - 16 ASCII characters.

STATUS	VARCHAR(17) ACTIVE (Default) Subscriber is active. TEMP-OOS Temporarily Out of Service. TEMP-DISCONNECTED Temporarily Disconnected. TEMP-UNAVAILABLE Temporarily Unavailable.
ADDRESS1	VARCHAR(32): 1 - 32 ASCII characters.
ADDRESS2	VARCHAR(32): 1 - 32 ASCII characters.
CITY	VARCHAR(16): 1 - 16 ASCII characters.
STATE	VARCHAR(16):1 - 16 ASCII characters.
COUNTRY	VARCHAR(16) Default = USA1 - 16 ASCII characters.
ZIPCODE	VARCHAR(10): 1 - 10 ASCII characters.
LANGUAGE	VARCHAR(16): 1 - 16 ASCII characters.
BILLING-DN	VARCHAR(14): 1 - 14 Numeric digits in the following format: NDC-EC-XXXX
DN1	UK VARCHAR(14):14 numeric digits in the NDC-EC-XXXX format.
PRIVACY	CHAR(4) NONE (Default) Display Name and Number. FULL Do not display name or number. NAME Do not display name. USER Use user-provided privacy information. Applies only to SIP endpoints that can include privacy information. If information is not received for either name or number, then privacy is indicated as “unspecified.”
RING-TYPE-DN1	CHAR(1)1, 2, OR 3Default = 1
MLHG-PREF-LIST-ID	FK MLGH-PREF-LIST TABLE.VARCHAR(16): 1 - 16 ASCII characters.
CTXG-ID	FK CENTREX-GRP TABLE. VARCHAR(16): 1 - 16 ASCII characters.
MLHG-ID	FK MLHG TABLE. VARCHAR(16): 1 - 16 ASCII characters.

TERM-TYPE	**VARCHAR(5): 1 – 5 ASCII characters** **TERM (Default):** **MGCP** **Termination ID** **TG** **Trunk Group** **ROUTE** **Route ID** **RG** **Route Guide ID** **SIP** **SIP Termination** **NONE** **There is no termination associated with the Subscriber.**
TERM-ID	**The TERM-ID and MGW-ID are used as a Termination ID. Use as a combined Foreign Key to the TERMINATION Table.** **FK TERMINATION TABLE.** **VARCHAR(32): 1 - 32 ASCII characters.**
MGW-ID	**VARCHAR(32): 1 - 32 ASCII characters.**
TGN-ID (or TG)	**FKTRUNK GROUP TABLE.** **INTEGER1 - 99999999**
POLICY_ID	**VARCHAR(16): 1 – 16 ASCII characters**
AOR_ID	**FK AOR2SUB TABLEVARCHAR(64)** **Use DOMAIN NAME** **PARSER RULES: Domain Name portion of AOR-ID exists in the Serving Domain Name Table**
MAC-ID (EMS ONLY)	**FK MAC2SUB TABLE** **VARCHAR(16): 1 – 16 ASCII Characters** **Only allowed if TERM-TYPE=SIPUSE UPPER CASE.**
PIC1	CHAR(4)NONE (Default) NPICXXXX (Numeric Digits)
PIC2	CHAR(4)NONE (Default) NPICXXXX (Numeric Digits)
PIC3	CHAR(4)NONE (Default) NPICXXXX (Numeric Digits)
GRP	CHAR(1)Y = GroupN (Default) = Individual
USAGE-SENS	CHAR(1) Y (Default) Allowed. N (NO) Usage sensitive features not allowed.

SUB-PROFILE-ID	FK SUBSCRIBER-PROFILE TABLE VARCHAR(16): 1 - 16 ASCII characters.
COS-RESTRICT-ID	FK COS-RESTRICT TABLE VARCHAR(16): 1 – 16 ASCII characters.
QOS-ID	FK VARCHAR(16): 1 - 16 ASCII characters.
IMMEDIATE-RELEASE	CHAR(1)Y / N (DEFAULT = N)
TERMINATING-IMMEDIATE-REL	CHAR(1)Y / N (DEFAULT = N)

Trigger ID

There is a new Trigger ID, REFER-TRIGGER.

Note New fields are in bold type.

Table 7 Trigger ID Table

Trigger ID	Description
ORIGINATION_ATTEMPT	
O_ATTEMPT_AUTHD	Origination Attempt Authorized.
VERTICAL_SERVICE_CODE	
CUSTOMIZE_DIALING_PLAN	
COS_TRIGGER	
911_TRIGGER	
LNP_TRIGGER	
SPECIFIC_DIGIT_STRING	
ROUTE_SELECT_FAILURE	
O_CALLED_PARTY_BUSY	
O_NO_ANSWER	
O_ANSWER	
O_SUSPEND	
O_REANSWER	
O_DISCONNECT	
O_ABANDON	
O_NOT_REACHABLE	
O_EXCEPTION	
O_SWITCH_HOOK_FLASH_IMMEDIATE	

Trigger ID	Description
REFER-TRIGGER	**REFER-TRIGGER is used by SIP for the Call Transfer feature.**
ROUTE_SELECTED	
TERMINATION_ATTEMPT	
TERMINATION_ATTEMPT_AUTHORIZED	
TERMINATION_RESOURCE_AVAILABLE	
CALL_ACCEPTED	
T_BUSY	
T_ANSWER	
T_NO_ANSWER	
T_SUSPEND	
T_REANSWER	
T_SWITCH_HOOK_FLASH_IMMEDIATE	
T_DISCONNECT	
T_ABANDON_DP	
T_NOT_REACHABLE	
T_EXCEPTION	
D_OF_TRIGGER	Not Used
ACCOUNT_CODE	Not Used
CNAM	
BLV	Busy Line Verification Trigger
SC1D-TRIGGER	1 Digit Speed Call Trigger
SC2D-TRIGGER	2 Digit Speed Call Trigger

Activity and Activity-Base

This section explains the changes to the activity table and the activity-base table for Release 4.5.x

Activity Table

In Release 4.5.x, the default value for the ENABLED token in the activity table is Y. Use the **delete activit**y command to disable the activities.

Activity-Base

Table 8 lists the ID token values for the activity-base table. The tokens related to SIA and SIM are new for Release 4.5.x.

Table 8 Activity Base ID Token Values Characteristics

ID	Valid-Freq	Fixed-Time Interval	So-Enabled	Restart-Enabled	Description
MEDIA- ALIVE-EM	6H, 8H, 12H, DAILY	N	N	N	Controls EM generation for long duration calls.
MGCP-TERM	30M, DAILY	N	Y	Y	Controls the trunking gateway MGCP-side CIC audit.
SIA-MEMORY-PERIODIC-AUDIT (Release 4.5)	15M, 30M, 1H, 2H, 3H,4H, 6H, 8H, 12H	N	Y	Y	SIA memory audit.
SIA-MEMORY-SCHEDULED-AUDIT (Release 4.5)	DAILY	N	N	N	Schedules an SIA memory audit daily at a fixed time.
SIM-MEMORY-PERIODIC-AUDIT (Release 4.5)	15M, 30M, 1H, 2H, 3H,4H, 6H, 8H, 12H	N	Y	Y	SIM memory audit.
SIM-MEMORY-SCHEDULED-AUDIT (Release 4.5)	DAILY	N	N	N	Schedules an SIM memory audit daily at a fixed time.
SS7-CIC		N	Y	Y	Controls the SS7-side CIC audit. Can be scheduled at any time.

New Tables

Address of Record to Subscriber

The Address of Record (AOR) to Subscriber (aor2sub) table is automatically provisioned when a subscriber is created. If a URL-based AOR is required, it can be manually provisioned using this table. This table is used for provisioning SIP telephones as subscribers.

Table 9 AOR2SUB Table Requirements

Table Name	AOR2SUB
Table Containment Area	Call Agent, EMS
Command Line Actions	Show, add, change, and delete

```
show aor2sub aor-id=joe@cisco.com;
change aor2sub aor-id=joe@cisco.com; sub-is=sub2;
change aor2sub status=INS; aor-id=4167940001@sia-SYS21CA146.ipclab.cisco.com;
```

Note In Release 4.5, the change command is used to control an aor2sub status. The control command is not supported.

Primary Key Token(s)	AOR-ID
Add Rules	None
Delete Rules	Can only be deleted if STATUS=OOS
Number of Instances	25,000

Table 10 AOR2SUB Syntax Description

* AOR-ID	Primary key. The AOR ID for the subscriber. VARCHAR(64): 1–64 ASCII characters.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.

SECURE-FQDN (Release 4.5)	Unique key. Specifies the secure-fqdn assigned to the AOR. Use a secure-fqdn to resolve an IP address and compare it with the IP address received from an endpoint during registration or during call setup (INVITE). VARCHAR(64): 1–64 ASCII characters. **Note** 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.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).
STATUS (System generated)	Status of the AOR. VARCHAR(16): 1–16 ASCII characters. INS—The AOR is in service. OOS—(Default) The AOR is out of service. **Note** This field is not provisionable. Use the status or control commands to change AOR status to INS or OOS. In Release 4.5, use the change command instead of the control command.
SUB-ID	Foreign key: Subscriber table. Subscriber ID. VARCHAR(30): 1–30 ASCII characters.

Authentication Realm

The Authentication Realm (auth-realm) table defines the authentication realm IDs supported by the Cisco BTS 10200 Softswitch. An auth-realm-id is assigned to subscribers using the Serving Domain Name table. All subscribers in a specific serving domain share a common auth-realm-id. This table is used primarily for SIP provisioning.

Table 11 AUTH-REALM Table Requirements

Table Name	AUTH-REALM
Table Containment Area	Call Agent
Command Line Actions	Show, add, change, and delete
show auth-realm id=rcdn-cisco; **add auth-realm id=rcdn-cisco; description=This realm id is for rcdn5 cisco.** **change auth-realm id=rcdn-cisco; description=This realm id is for all of cisco in Richardson.** **delete auth-realm id=rcdn-cisco;**	
Primary Key Token(s)	ID
Add Rules	None
Change Rules	None
Delete Rules	FK constraints
Number of Instances	Equal to number of Centrex groups.

Table 12 AUTH-REALM Syntax Description

* ID	Primary key. The realm ID. VARCHAR(64): 1–64 ASCII characters.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DESCRIPTION	Described by the service provider. VARCHAR(64): 1–64 ASCII characters.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

MAC to Subscriber

Note Provisioning this table is not required for phones without GUI capability.

For multi-line SIP phones like the Cisco 7960, the MAC2SUB table is provisioned for only one of the lines. The GUI feature for controlling call forwarding is provided only for that line.

The MAC to Subscriber (mac2sub) table links the MAC Address of a device to a subscriber ID. This table is automatically provisioned when a MAC device is associated with a subscriber. This table is used primarily for SIP provisioning.

Table 13 MAC2SUB Table Requirements

Table Name	MAC2SUB
Table Containment Area	PTC Feature Server
Command Line Actions	Show, add, change, and delete

`show mac2sub mac-id=SIP0002B9A74E4C;`
`add mac2sub mac-id=SIP0002B9A74E4C; sub-id=sub1;`
`delete mac2sub mac-id=SIP0002B9A74E4C;`
`change mac2sub MAC_ID=SIP000BBE3718A0; sub-id=sub9`	

Primary Key Token(s)	MAC-ID
Add Rules	None
Delete Rules	None
Number of Instances	25,000

Table 14 MAC2SUB Syntax Description

* MAC-ID	Primary key. MAC ID (Mac Address) of the IP Phone or device. VARCHAR(16): 1–16 ASCII characters.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.

ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).
SUB-ID	Foreign key: Subscriber table. Subscriber ID. Assigned by service provider. VARCHAR(30): 1–30 ASCII characters.

Serving Domain Name

The Serving Domain Name (serving-domain-name) table defines serving domain names supported by the Cisco BTS 10200 Softswitch. This table is also used to define authentication requirements for subscribers served by the serving domain. This table is used primarily for Session Initiation Protocol (SIP) provisioning.

Note The domain name value must resolve in the DNS to the logical IP addresses, designated for use by the SIP adaptor during installation of the Cisco BTS 10200 system. The resolution for the serving domain must be identical to the resolution of the FQDN specified as the Cisco BTS 10200 contact.

Table 15 SERVING-DOMAIN-NAME Table Requirements

Table Name	SERVING-DOMAIN-NAME
Table Containment Area	Call Agent, EMS
Command Line Actions	Show, add, change, and delete
show serving-domain-name; **add serving-domain-name domain-name=rcdn.cisco.com; auth-realm-id=rcdn-cisco; auth-reqd=Y;** **change serving-domain-name domain-name=rcdn.cisco.com; auth-realm-id=" "; auth-reqd=N;** **delete serving-domain-name domain-name=rcdn.cisco.com;**	
Primary Key Token(s)	domain-name
Add Rules	AUTH-REALM-ID IS REQUIRED IF AUTH-REQD=Y AUTH-REALM-ID IS NULL IF AUTH-REQD=N
Change Rules	Same as add rules.
Delete Rules	FK constraints
Number of Instances	Equal to number of Centrex groups.

Table 16 SERVING-DOMAIN-NAME Syntax Description

* DOMAIN-NAME	Primary key. The domain name supported by the Cisco BTS 10200 Softswitch. This field is case insensitive. VARCHAR(64): 1–64 ASCII characters.
AUTH-REALM-ID	Foreign key: Authentication Realm table. Specifies the Auth Realm ID to be used if authentication is required. VARCHAR(64): 1–64 ASCII characters. **Note** auth-realm-id is required if auth-reqd=Y auth-realm-id is null if auth-reqd=N
AUTH-REQD	Specifies whether SIP messages from the serving domain must be authenticated or not. CHAR(1): Y/N (Default = Y).
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DESCRIPTION	Described by the service provider. VARCHAR(64): 1–64 ASCII characters.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

User Authentication

The User Authentication (user-auth) table identifies the subscriber address of record (AOR) based on the authentication credentials supplied by the user during registration or call setup. When a SIP user attempts to register or set up a call, the Cisco BTS 10200 Softswitch challenges the SIP subscriber based on information from the Serving Domain Name table. If the Serving Domain Name Table indicates that authentication is required, the Cisco BTS 10200 Softswitch challenges the SIP user to send a user ID and password (HA1) based on the auth-realm-id. If the Cisco BTS 10200 Softswitch receives a valid user ID and password, the AOR in this table is used to identify the subscriber based on the AOR to Subscriber table.

Table 17 USER-AUTH Table Requirements

Table Name	USER-AUTH
Table Containment Area	Call Agent, EMS
Command Line Actions	Show, add, change, and delete

`show user-auth auth-user=joe; auth-realm-id=rcdn-cisco;`
`add user-auth auth-user=joe; auth-realm-id=rcdn-cisco; password=mhallwfmesw;`
`aor-id=joe@rcdn.cisco.com`
`change user-auth auth-user-joe;password=joe2seven;`
`delete user-auth auth-user=joe; auth-realm-id=rcdn-cisco;`	

Primary Key Token(s)	AUTH-USER, AUTH-REALM-ID
Add Rules	None
Delete Rules	None
Number of Instances	25,000

Table 18 USER-AUTH Syntax Description

* AUTH-USER	Primary key. The authentication user name. VARCHAR(32): 1–32 ASCII characters.
AOR-ID	Foreign key: AOR to Subscriber table. The aor-id. VARCHAR(64): 1–64 ASCII characters.
AUTH-REALM-ID	Primary key. The authentication realm id. VARCHAR(64): 1–64 ASCII characters.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.

HA1	Represents a Hashed Password–MD5 of USER:REALM:PASSWORD according to RFC 2617. This value is computed and automatically provisioned by the Element Management System. CHAR(32): 1–32 characters.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
PASSWORD	The password for this auth-user. VARCHAR(64): Not stored.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

Note For SIP phone Authentication:
The Auth-Realm table must be provisioned and authentication_reqd set to Y in the Serving Domain Table. The user-auth table must be provisioned with the same user/password as specified in the linex specification inside the config file for the phone.

SIP Timer Profile

The Session Initiation Protocol (SIP) Timer Profile (sip-timer-profile) table defines a SIP timer profile for a Softswitch Trunk Group Profile or a default SIP timer profile at the system level.

Caution Deviation from default timer values can significantly influence system performance and reliability. Exercise great caution and consult with Cisco TAC prior to making changes.

Table 19

* ID (Release 4.5)	Primary key. Identifies the primary key of the records in this table. VARCHAR(16): 1–16 ASCII characters.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
INVITE-INCOMPLETE-TIMER-SECS	Specifies whether to clean up user agent client (UAC) invite transactions when a provisional response of less than 180 is received, but no ringing or final response is received within a reasonable period of time. INTEGER: 15–600 (Default = 40).
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
MIN-SE (Release 4.5)	Specifies the minimum number of session-expires allowed, in seconds, to be sent or received. INTEGER: 100–1800 (Default = 900).
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
SESSION-EXPIRES-DELTA-SECS (Release 4.5)	SIP session timer, in seconds, for SIP auditing purposes. Specifies when to send a periodic refresh for each session to check the liveness of the session. This conveys the session interval for a SIP call. INTEGER: 100–7200 (Default = 1800).
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

Table 19

TIMER-A-MILLI (Release 4.5)	The SIP RFC3261 timer, in milliseconds, for the INVITE request retransmit interval, for User Datagram Protocol (UDP) only. INTEGER: 0, 100–5000 (Default = 0). **Note** A default value of zero means that values for those timers are computed automatically from TimerT1, TimerT2, and TimerT4.
TIMER-B-SECS (Release 4.5)	The SIP RFC3261 timer, in seconds, for INVITE transaction timeout. INTEGER: 0–3600 (Default = 0). **Note** A default value of zero means that values for those timers are computed automatically from TimerT1, TimerT2, and TimerT4.
TIMER-D-SECS (Release 4.5)	The SIP RFC3261 timer, in seconds, for the wait time for response retransmits. INTEGER: 33–65 (Default = 33).
TIMER-E-MILLI (Release 4.5)	The SIP RFC3261 timer, in milliseconds, for non-INVITE request retransmit interval, UDP only. INTEGER: 0, 100–5000 (Default = 0). **Note** A default value of zero means that values for those timers are computed automatically from TimerT1, TimerT2, and TimerT4.
TIMER-F-SECS (Release 4.5)	The SIP RFC3261 timer, in seconds, for non-INVITE transaction timeout. INTEGER: 0–3600 (Default = 0). **Note** A default value of zero means that values for those timers are computed automatically from TimerT1, TimerT2, and TimerT4.
TIMER-G-MILLI (Release 4.5)	The SIP RFC3261 timer, in milliseconds, for INVITE response retransmit interval. INTEGER: 0, 100–5000 (Default = 0). **Note** A default value of zero means that values for those timers are computed automatically from TimerT1, TimerT2 and TimerT4.
TIMER-H-SECS (Release 4.5)	The SIP RFC3261 timer in seconds for the wait time for ACK receipt. INTEGER: 0–3600 (Default = 0). **Note** A default value of zero means that values for those timers are computed automatically from TimerT1, TimerT2, and TimerT4.

Table 19

TIMER-I-SECS (Release 4.5)	The SIP RFC3261 timer in seconds for wait time for ACK retransmits. INTEGER: 0–10 (Default = 0) **Note** A default value of zero means that values for those timers are computed automatically from TimerT1, TimerT2, and TimerT4.
TIMER-J-SECS	The SIP RFC3261 timer in seconds for wait time for non-INVITE request retransmits. INTEGER: 0–3600 (Default = 0) **Note** NOTE: Default value of zero means that values for those timers will be computed automatically from TimerT1, TimerT2 and TimerT4.
TIMER-T1-MILLI (Release 4.5)	Specifies the SIP RFC3261 timer, in milliseconds, for RTT estimate. INTEGER: 100–5000 (Default = 500).
TIMER-T2-SECS (Release 4.5)	Specifies the SIP RFC3261 timer, in seconds, for the maximum retransmit interval for SIP non-INVITE requests and INVITE responses. INTEGER: 1–10 (Default = 4).
TIMER-T4-SECS (Release 4.5)	The SIP RFC3261 timer, in seconds, for the maximum duration a SIP message remains in the network. INTEGER: 1–10 (Default = 5).

SIP Adaptor Configuration Parameters (CA-CONFIG)

The CA-CONFIG table has parameters that users can specify in order to influence the behavior and features provided by Cisco BTS 10200. Table 20 contains the parameters and their description, for the Cisco BTS 10200 SIP Adaptor. Table 1 contains those parameters and their descriptions that are applicable to the SIP Adaptor in the Cisco BTS 10200.

The default values in Table 20 are implemented in the Cisco BTS 10200 software when the corresponding parameter is not provisioned in the CA-CONFIG table. The entries must be provisioned only if the values are required to differ from the default.

For more information about the CA-CONFIG table, refer to the Call Agent Configuration section in the *Cisco BTS 10200 Softswitch Command Line Interface* guide.

The following items were added in Release 4.x:

- REFER-ACCEPT-TIMER-SECS
- REFER-ABANDON-TIMER- SECS
- NONCE-LIFETIME
- MIN-SE
- MAX-SESSION-EXPIRES
- SESSION-EXPIRES
- SIA-REGISTER-DEFAULT- EXPIRES
- SIA-REG-MIN-EXPIRES-SECS
- SIA-REG-MAX-EXPIRES- SECS
- SUB-SESSION-TIMER- ALLOWED

Note The CHK-POS-VAL field in Table 20 is a new capability added to Release 4.1. If a token is defined as a “string,” you now can specify possible values for that string, and EMS checks the possible values before allowing change/add for the CA-CONFIG parameter.

Note New fields are in bold type.

Table 20 Configuration Parameters for the Cisco BTS 10200 SIP Adaptor

TYPE	DATA TYPE	FROM-VALUE	TO-VALUE	CHK-POS-VAL	DEFAULT	DESCRIPTION
MAX-3XX-COUNT	Integer	1	5	N	1	Maximum 3XX (Redirection) allowed.
MAX-SESSION-EXPIRES	Integer	1800	7200	N	7200	Maximum session expiry in seconds. This SIP feature session timer is for SIP auditing purposes. A periodic refresh is sent for each session to check the liveness of the session. This conveys the session interval for a SIP call.
MAX-SUBSCRIPTION-LEVEL	Integer			N	3600	The notifier can choose to limit/lower the duration of a subscription that is requested by the subscriber (in seconds).
MIN-SE	Integer	900	1800	N	900	In seconds. This is the minimum session-expires allows to be sent or received.
NONCE-LIFETIME	Integer	0		N	180	Limits replay attacks and masquerades by setting an upper limit for the duration of validity of a nonce sent out in a challenge. It is specified in seconds. A value of 0 implies one-time nonces should be used (for example, each request is challenged with a new nonce). No Upper Limit.
REFER-ABANDON-TIMER-SECS	Integer			N	180	Seconds to wait before giving up on a Transfer request and sending a failure Notification to the transferee. (No RANGE is specified.)
REFER-ACCEPT-TIMER-SECS	Integer			N	10	Seconds to wait for response from BCM/FS before rejecting a Refer request. (No RANGE is specified.)
SESSION-EXPIRES	Integer	1800	7200	N	1800	(In seconds) This SIP feature -Session timer is for SIP auditing purposes. A periodic refresh is sent for each session to check the liveness of the session. This conveys the session interval for a SIP call.
SIA-REGISTER-DEFAULT-EXPIRES	Integer	3600		N	3600	(In seconds) A register request may be received without any expires parameter. Cisco BTS 10200 uses this value to set the expires value for that Registration. No Upper Limit.

TYPE	DATA TYPE	FROM-VALUE	TO-VALUE	CHK-POS-VAL	DEFAULT	DESCRIPTION
SIA-REG-MAX-EXPIRES-SECS	Integer			N	7200	Used by the Registrar to restrict the Maximum value for Contact expiration.
SIA-REG-MIN-EXPIRES-SECS	Integer	1800		N		Registrar rejects the register request having a value less than 3600 and less than MIN_EXPIRES. There is no upper limit.
SIA-SIG-TOS-LOWDELAY	Boolean			N	Y	Specifies whether to set this socket option, signalling (SIG) type of service (ToS) low delay (LOWDELAY) to 1 (Y) or 0 (N). Low delay refers to the waiting time, or latency involved in sending and receiving a packet. You can set various options on the TCP socket to tune or optimize for certain performance parameters. **Note** Cisco does not recommend using any value other than the specified default. Changing this value from its default may significantly impact network performance. Contact Cisco TAC for further information.

TYPE	DATA TYPE	FROM-VALUE	TO-VALUE	CHK-POS-VAL	DEFAULT	DESCRIPTION
SIA-SIG-TOS-PRECEDENCE	Integer	0	7	N	3	Specifies the designation assigned to a phone call by the caller to indicate the relative urgency (and thus the order of handling) of a call. It also sends an indication to the called party of the order in which the call is answered. Values are: • NETCONTROL (=7) • INTERNETCONTROL (=6) • CRITICAL (=5) • FLASHOVERRIDE (=4) • FLASH (DEFAULT=3) • IMMEDIATE (=2) • PRIORITY (=1) • ROUTINE (=0) **Note** Cisco does not recommend using any value other than the specified default. Changing this value from its default may significantly impact network performance. Contact Cisco TAC for further information.
SIA-SIG-TOS-RELIABILITY	Boolean			N	N	Specifies whether to set this socket option, signalling (SIG) type of service (ToS) reliability (RELIABILITY) to 1 (Y) or 0 (N). Reliability refers to the dependability of packet delivery. **Note** Cisco does not recommend using any value other than the specified default. Changing this value from its default may significantly impact network performance. Contact Cisco TAC for further information.

TYPE	DATA TYPE	FROM-VALUE	TO-VALUE	CHK-POS-VAL	DEFAULT	DESCRIPTION
SIA-SIG-TOS-THROUGHPUT	Boolean			N	N	Specifies whether to set this socket option, media gateway adaptor (MGA) signaling (SIG) type of service (ToS) throughput (THROUGHPUT) to 1 (Y) or 0 (N). Throughput refers to the actual amount of useful and non-redundant information that is transmitted or processed. The relationship between what went in one end of the network and what came out the other is a measure of the efficiency of that communications network. Throughput is a function of bandwidth, error performance, congestion, and other factors. **Note** Cisco does not recommend using any value other than the specified default. Changing this value from its default may significantly impact network performance. Contact Cisco TAC for further information.
SIA-TRUNK-GRP-LEVEL-SIG-TOS	Boolean			N	N	The SIA SIG ToS values define the system level ToS used for SIP calls. If the flag is set to Y, the system reads the TG level SIG ToS values and overrides the system level ToS values if required. If this token is set to Y, system level ToS tokens are still set. System level ToS tokens are used when sending messages when the trunk group is not known.
SUB-SESSION-TIMER-ALLOWED	Boolean			N	N	This flag controls the session timer feature for all Cisco BTS 10200 SIP Subscribers. When TRUE, session timer is activated on every call to/from a SIP subscriber.

CHAPTER 6

Measurements, Events, and Alarms

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

This section describes the new Release 4.5.x measurements, events, and alarms related to the SIP protocol. For more complete information on these topics, see the following documents:

- For CLI information, see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide.*
- For a full list of measurements, see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.
- For complete information on events and alarms, see the *Cisco BTS 10200 Softswitch Troubleshooting Guide*.

Measurements

In this release, the following counters were renamed:

- The common SIP counters were renamed from SIP_ to SIS_.
- The application-specific SIA counters were renamed from SIP_ to SIA_.
- The SIP audit counters were renamed from AUDIT_SIP to SIA_AUDIT.
- The SIM audit counters were renamed from AUDIT_SIM to SIM_AUDIT.

The SIP memory audit counters were removed from the AUDIT category

The following counters were added to the SIA category:

- SIA_AUDIT_CCB_FREED
- SIA_AUDIT_CALL_RELEASED
- SIA_AUDIT_BCM_CALL_RELEASED
- SIA_AUDIT_REGCONTACT_FREED

The following counters were added to the SIM category:

- SIM_AUDIT_CCB_FREED
- SIM_AUDIT_SIP_CCB_FREED

The following SIA counters were deprecated; they will still be displayed in this release, but they will always contain a value of zero:

- SIA_TOTAL_SUCC

- SIA_TOTAL_FAIL
- SIA_TOTAL_OUTG_MSG_FAIL
- SIA_TOTAL_INCOM_MSG_FAIL

The following security-related measurements were added to the SIP Interface Adapter category.

- SIA_SECURE_FQDN_VIOLATION_REQ
- SIA_SECURE_FQDN_VIOLATION_RESP

The following T.38 fax-related measurements were added to the Call Processing category:

- CALLP_T38_FAX_MEDIA_SETUP_SUCC
- CALLP_T38_FAX_MEDIA_SETUP_FAIL

Events and Alarms

The following SIP-related events and alarms were introduced in Release 4.5.x.

- SECURITY(6)—Secure SIP endpoint validation failure, WARNING
- SIGNALING(146)—All retransmission attempts of SIP request or response failed, WARNING
- SIGNALING(147)—DNS SRV addresses exhausted, WARNING

MGCP Features vs. SIP Features

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

The SIP support features provided in Release 4.5.x were built on the existing Cisco BTS 10200 Softswitch software and hardware platform. Table A-1 lists the MGCP features available (in the Feature column) and then describes how the feature differs when used as a SIP feature.

Table A-1 MGCP Features and SIP Support

Feature	Abbreviation	Support for SIP Phone Endpoint
Emergency-Service	911	Only E911 support (without the suspend procedure for 45 minutes). Basic 911 with suspend procedure is not supported.
Toll-Free	8xx	Same as MGCP.
Anonymous Call Rejection	ACR	Same as MGCP, when provided by Cisco BTS 10200. Also provided by the phone.
Cancel-Call-Waiting	CCW	Functionality provided by the phone. Cisco BTS 10200 supports the interface.
Call-Forward-Busy	CFB	Same as MGCP.
Call-Forward-No-Answer	CFNA	Same as MGCP.
Call-Forward-Unconditional	CFU	Same as MGCP.
Calling-Identity-Delivery Suppression	CIDSD	Presentation status from the phone, and single stage digit collection.
Calling Name Delivery Blocking	CNAB	Presentation status from the phone, and single stage digit collection.
Calling Name Delivery	CNAM	Same as MGCP.
Calling Number Delivery	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.

Table A-1 MGCP Features and SIP Support

Feature	Abbreviation	Support for SIP Phone Endpoint
Calling Number Delivery Blocking	CNDB	Presentation status from the phone, and single stage digit collection.
Class-of-Service	COS	CoS Screening supported, without Auth/Account code collection.
Call-Transfer	CT	For SIP phones, this feature is provided as part of REFER support on the Cisco BTS 10200. See REFER feature for more details.
Call-waiting	CW	Functionality provided by the phone. Cisco BTS 10200 supports the interface.
Number Portability	LNP	Same as MGCP.
Three-way-Call	TWC	Functionality provided by the phone. Cisco BTS 10200 supports the interface.
Usage-Sensitive-Three-way-call	USTWC	Functionality provided by the phone. Cisco BTS 10200 supports the interface.
Custom-Dial-Plan	CDP	Same as MGCP.
Call-Hold	CHD	Functionality provided by the phone. Cisco BTS 10200 supports the interface.
Calling Identity Delivery on Call Waiting	CIDCW	Functionality provided by the phone. Cisco BTS 10200 supports the interface.
Incoming-Simulated-Facility-Group	ISFG	Same as MGCP.
Outgoing-Simulated-Facility-Group	OSFG	Same as MGCP.
Automatic Callback	AC	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Automatic Callback	AC_ACT	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Automatic Callback	AC_DEACT	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Anonymous Call Rejection	ACR_ACT	Cisco BTS 10200 supported functionality is same as MGCP, and also through the phone's "Services" key. There's another method of activating the service supported by the phone itself.
Anonymous Call Rejection	ACR_DEACT	Cisco BTS 10200 supported functionality is same as MGCP, and also through the phone's "Services" key. There's another method of deactivating the service supported by the phone itself.

Table A-1 MGCP Features and SIP Support

Feature	Abbreviation	Support for SIP Phone Endpoint
Automatic Recall	AR	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Automatic Recall	AR_ACT	SIP phone users cannot activate the service. MGCP users cannot activate the service toward SIP phone users.
Automatic Recall	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.
Customer Originated Trace	COT	Same as MGCP.
Call-Park	CPRK	Not supported.
Call-Park	CPRK_RET	Not supported.
Distinctive Alerting Call Waiting Indication	DACWI	Ringing part supported by Cisco BTS 10200. The Cisco BTS 10200 sends distinctive alerting request for Call-Waiting scenario; some SIP phones can interpret it and play a distinctive call-waiting tone, while other phones do not.
Directed Call Pickup - without Barge-in	DPN	Not supported.
Directed Call Pickup - with Barge-in	DPU	Not supported.
Distinctive Ringing Call Waiting	DRCW	Ringing part supported by Cisco BTS 10200. The Cisco BTS 10200 sends a distinctive alerting request for a Call-Waiting scenario. Some SIP phones interpret it and play distinctive call-waiting tone, while other SIP phones do not.
Distinctive Ringing Call Waiting	DRCW_ACT	Same as MGCP.
Hotline	HOTLINE	Not supported.
Multiple Directory Number	MDN	Ringing part supported by Cisco BTS 10200. The Cisco BTS 10200 sends a distinctive alerting request for a Call-Waiting scenario. Some SIP phones interpret it and play distinctive call-waiting tone, while other SIP phones do not.
Remote Activation of Call Forwarding	RACF	Same as MGCP.
Remote Activation of Call Forwarding	RACF_PIN	Same as MGCP.

Table A-1 MGCP Features and SIP Support

Feature	Abbreviation	Support for SIP Phone Endpoint
Selective Call Acceptance	SCA	Same as MGCP.
Selective Call Acceptance	SCA_ACT	Same as MGCP.
Selective Call Forwarding	SCF	Same as MGCP.
Selective Call Forwarding	SCF_ACT	Same as MGCP.
Selective Call Rejection	SCR	Same as MGCP.
Selective Call Rejection	SCR_ACT	Same as MGCP.
Warmline	WARMLINE	Not supported.
Do Not Disturb	DND	Same as MGCP.
Do Not Disturb	DND_ACT	Same as MGCP, and also available through the phone's "Services" key.
Do Not Disturb	DND_DEACT	Same as MGCP, and also available through the phone's "Services" key.
Group Speed Call - 1 digit	GSC1D	Not supported.
Group Speed Call - 2 digit	GSC2D	Not supported.
Speed Call - 1 digit	SC1D	Not supported.
Speed Call - 1 digit	SC1D_ACT	Not supported.
Speed Call - 2 digit	SC2D	Not supported.
Speed Call - 2 digit	SC2D_ACT	Not supported.
Call Block	CBLK	Same as MGCP.
Calling-Identity-Delivery Suppression	CIDSS	Presentation status from the phone, and single stage digit collection.
Call-Forward-Busy	CFBI	Single stage digit collection.
Call-Forward-No-Answer	CFNAI	Single stage digit collection.
Call-Forward-Unconditional	CFUI	Single stage digit collection.
Call-Waiting Deluxe	CWD	Varies with phone functionality.
Call-Waiting Deluxe	CWDA	Varies with phone functionality.
Call-Waiting Deluxe	CWDD	Varies with phone functionality.
Call-Waiting Deluxe	CWDI	Varies with phone functionality.
Hotline-Variable	HOTV	Not supported.
Hotline-Variable	HOTVA	Not supported.
Hotline-Variable	HOTVD	Not supported.
Hotline-Variable	HOTVI	Not supported.
Outgoing Call Barring	OCB	Same as MGCP.
Outgoing Call Barring	OCBA	Single stage digit collection, and also through the phone's "Services" key.
Outgoing Call Barring	OCBD	Single stage digit collection, and also through the phone's "Services" key.

Table A-1 MGCP Features and SIP Support

Feature	Abbreviation	Support for SIP Phone Endpoint
Outgoing Call Barring	OCBI	Single stage digit collection, and also through the phone's "Services" key.
Three-way-Call Deluxe	TWCD	Varies with phone functionality.
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.
Call-Forward-Busy	CFBVA	Single stage digit collection, and also through the phone's "Services" key.
Call-Forward-Busy	CFBVD	Same as MGCP, and also available through the phone's "Services" key.
Call-Forward-No-Answer	CFNAVA	Single stage digit collection, and also through the phone's "Services" key.
Call-Forward-No-Answer	CFNAVD	Same as MGCP, and also available through the phone's "Services" key.
Call-Forward-Unconditional	CFUA	Single stage digit collection, and also through the phone's "Services" key.
Call-Forward-Unconditional	CFUD	Same as MGCP, and also available through the phone's "Services" key.

A

AC	automatic callback
AC_ACT	automatic callback activation
AC_DEACT	automatic callback deactivation
ACR	anonymous call rejection
ACR_ACT	anonymous call rejection activation
ACR_DEACT	anonymous call rejection deactivation
AI	asserted identity
ANI	automatic number identification
AOR	address of record
AOR2SUB	Address of Record to Subscriber (refers to new table)
AR	automatic recall
AR_ACT	automatic recall activation
AR_DEACT	automatic recall deactivation
ATA	analog telephone adaptor
AUTH-REALM	Authentication Realm (refers to new table)

B

BCM	Basic Call module
BGID	Business Group Identity
BLV	Busy Line Verification

C

CA	Call Agent

CA-CONFIG	Call Agent configuration (refer to the SIP Adapter Configuration Parameters table)
CALEA	Communications Assistance for Law Enforcement Act
CAS	channel-associated signaling
CAT	customer access treatment
CBLK	call block (reject caller)
CCW	cancel call waiting
CDP	custom dial plan
CDR	call detail record
CF	call forwarding
CFB	call forwarding on busy
CFBI	call forwarding on busy interrogation
CFBVA	call forwarding on busy variable activation
CFBVD	call forwarding on busy variable deactivation
CFNA	call forwarding on no answer
CFNAI	call forwarding on no answer interrogation
CFNAVA	call forwarding on no answer variable activation
CFNAVD	call forwarding on no answer variable deactivation
CFU	call forwarding unconditional
CFUA	call forwarding unconditional activation
CFUD	call forwarding unconditional deactivation
CFUI	call forwarding unconditional interrogation
CHD	call hold
CIC	circuit identification code, carrier identification code
CID	calling identity delivery, also caller ID (see also CND)
CIDB	calling identity delivery blocking
CIDCW	calling identity delivery on call waiting
CIDS	calling identity delivery and suppression (per call)
CIDSD	calling identity delivery and suppression (per call)—delivery part

CIDSS	calling identity delivery and suppression (per call)—suppression part
CLASS	custom local area signaling services
CLI	command-line interface
CMSS	Call Management System Signaling
CNAB	calling name delivery blocking
CNAM	calling name delivery
CND	calling number delivery, calling number display
CNDB	calling number delivery blocking
CODEC	coder/decoder, compression/decompression
COS	class of service
COT	customer-originated trace, continuity testing, central office termination
CPT	called party termination
CPRK	call park
CPRK_RET	call park retrieve
CT	call transfer, call type
CW	call waiting
CWD	call waiting deluxe
CWDA	call waiting deluxe activation
CWDD	call waiting deluxe deactivation
CWDI	call waiting deluxe interrogation
CWI	call waiting indication

D

DACWI	distinctive alerting call waiting indication
DPN	directed call pickup without barge-in
DPU	directed call pickup with barge-in
DID	direct inward dialing
DN	directory number

DND do not disturb

DND_ACT do not disturb activation

DND_DEACT do not disturb deactivation

DNS domain name server

DNS SRV domain name server services

DOD direct outward dialing

DP dial plan

DPN directed call pickup without barge-in

DPN_O directed call pickup without barge-in (originate)

DPN_T directed call pickup without barge-in (terminate)

DPU directed call pick-up with barge-in

DPU_O directed call pickup with barge-in (originate)

DPU_T directed call pickup with barge-in (terminate)

DRCW distinctive ringing/call waiting

DRCW_ACT distinctive ringing/call waiting activation

DTMF dual tone multifrequency

E

E.164 Telephone number standard of ITU

E-911 Enhanced 911

EMS Element Management System

F

FDT Final Stage Dial Tone

FS Feature Server

FQDN fully qualified domain name

G

GAP generic address parameter

GUI graphical user interface

GUI FS graphical user interface feature server

H

H.323 ITU-T recommendation adopted by the VoIP Forum as the call signaling protocol over LAN

HOTLINE hotline

HTML HyperText Markup Language

HTTP Hypertext Transfer Protocol

I

IETF Internet Engineering Task Force

INS in service

IP Internet Protocol

ISDN Integrated Services Digital Network

ISFG Incoming simulated facility group

ISUP ISDN user part

ITP IP transfer point

IVR interactive voice response

J

K

L

LATA local access and transport area

LNP local number portability

LSSGR LATA Switching Systems Generic Requirements

M

MAC2SUB MAC to Subscriber (refers to new table)

MDN multiple directory numbers

MF multifrequency

MG (MGW) media gateway

MGCP Media Gateway Control Protocol

MGW (MG) media gateway

MLHG multiline hunt group

MWI message waiting indicator

N

NAPTR Naming Authority Pointer

NP number portability

NPDI number portability dip indication

O

OAM operations, administration, and maintenance, Operations administration module

OCB outgoing call barring

OCBA outgoing call barring activation

OCBD outgoing call barring deactivation

OCBI outgoing call barring interrogation

OOS out of service

OSFG outgoing simulated facility group

P

POTS plain old telephone service

PRACK provisional response acknowledgement

PRI primary rate interface

PSTN public switched telephone network

Q

QoS quality of service

R

RACF remote activation of call forwarding

RACF-PIN remote activation of call forwarding personal ID number

RFC Request for Comment (IETF)

RQNT request for notification

RN routing number

S

SC1D speed call 1-digit

SC1D_ACT speed call 2-digit activation

SC2D speed call 1-digit

SC2D_ACT speed call 2-digit activation

SCA selective call acceptance

SCA_ACT selective call acceptance activation

SCF selective call forwarding

SCF_ACT selective call forwarding activation

SCR selective call rejection

SCR_ACT selective call rejection activation

SDP Session Description Protocol

SIA	SIP adapter
SIP	Session Initiation Protocol
SIP-T	SIP for telephones
SLE	screening list editing
SP	service provider
SPCS	stored program control system
SRV	server resource records
SS7	Signaling System 7

T

TCP	Transmission Control Protocol
TF	toll free
TG	trunk group
TGID	trunk group identity
TGW	trunking gateway
ToS	type of service
TSAP	Transport Service Access Point
TWC	three-way calling
TWCD	three-way calling deluxe

U

UAC user agent client

UAS user agent server

UDP User Datagram Protocol

UI user interface

URI uniform resource identifier

URL universal resource locator

USER-AUTH User Authentication (refers to new table)

USTWC usage-sensitive three-way calling

V

VM voice mail

VoIP voice over IP

VSC vertical service code

W

WARMLINE warmline

WFI waiting for instruction

X

***x*DSL** (generic) digital subscriber line

Y

Z