Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions

March 24, 2011

Americas 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: 408 527-0883

Text Part Number: OL-12606-21

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions
Copyright © 2011 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface ix

Conventions ix

Updates to this Document for Release 5.0 x

Obtaining Documentation, Obtaining Support, and Security Guidelines xiii

CHAPTER 1 **Network Features** 1-1

Interoperability 1-2

Numbering Plans and Dialing Procedures 1-2

Digit Manipulation 1-3

E.164 Dialing Plan Implementation 1-3

Casual Dialing (Dial Around) 1-5

Dial 1 Options for Local, Toll, and InterLATA Calls 1-5

Directory Services (411, 555-1212, 0+ Listing Services) 1-5

Easily Recognizable Codes 1-6

Information Service Calls (900 and 976) 1-6

n11 support (211, 311, 411, 511, 611, 711, 811) 1-6

NRUF Reporting for NANPA Audit Support 1-8

Emergency Services (911) 1-8

Description 1-8

Important Provisioning Requirements 1-9

911 Overflow Announcement 1-10

Emergency 911 Trunk Connection Loss Alarm 1-10

Feature Interactions 1-10

Feature Provisioning Commands 1-10

Operator Services 1-11

Numbers Used to Access Operator Services 1-11

Types of Services 1-11

Busy Line Verification (BLV) and Operator Interrupt (OI) Services 1-12

Network Services 1-13

8XX (Toll-Free Calling) 1-13

Active Call Information Display 1-16

Alerting Notification to Third-Party Feature Server 1-17

Calling Party Number Options for Outgoing SETUP Messages 1-19

Dialing Parity (IntraLATA Toll Presubscription) 1-22

Local Number Portability (LNP) 1-23
RFC 2833 DTMF Relay—Call Agent Controlled Mode 1-24
SIP Triggers 1-26
Split-NPA 1-38
T.38 Fax Relay, Modem, and TDD Handling 1-38
CMTS Discovery Using the Static Subnet Table 1-46
Aggregation Id Subnet 1-47
ENUM Capability 1-47
Trunk and Line Testing 1-57
Trunk Testing 1-58
Testing Capability for 911 FGD-OS Trunks 1-60
Network Loopback Test for NCS/MGCP Subscriber Endpoints 1-60
Network Loopback Test for ISDN PRI Trunks 1-61

CHAPTER 2 **Lawful Intercept and Enhanced CALEA Features** 2-1
General Description of Lawful Intercept Implementation 2-1
Lawful Intercept Provisioning Interface 2-1
Lawful Intercept Call Data Interface 2-2
Lawful Intercept Call Content Function 2-2
Enhanced CALEA Features 2-2
CALEA Enhancement Overview 2-3
Generic CALEA Enhancements 2-3
Surveillance for Calls Involving Multiple CMSs 2-4
BTS 10200 CALEA Interaction with SIP Endpoints 2-6
Changes to Interface between the BTS 10200 and Delivery Function Server 2-7
BTS 10200 CALEA Interaction with SIP Triggers Feature 2-9
CALEA Backward Compatibility 2-10
Compliance with CALEA Requirements in PKT-SP-EM1.5-I01-050128 Appendix A 2-12
Compliance with CALEA Requirements in PKT-SP-CMSS1.5-I01-050128 Section 7.7.2 2-17

CHAPTER 3 **Subscriber Features** 3-1
Interoperability 3-2
Subscriber Feature List 3-2
Call Forwarding Features 3-6
Call Forwarding Unconditional (CFU) 3-7
Call Forwarding Variable for Basic Business Group (CFVBBG) 3-13
Remote Activation of Call Forwarding (RACF) 3-15
Remote Call Forwarding (RCF) 3-16
Call Forwarding Busy (CFB) 3-16

Call Forwarding No Answer (CFNA) 3-23
Call Forwarding Combination (CFC) 3-31
Call Waiting Features 3-39
Limitations 3-39
Call Waiting (CW) 3-40
Cancel Call Waiting (CCW) 3-42
Calling Identity Delivery on Call Waiting (CIDCW) 3-43
Call Waiting Deluxe (CWD) 3-45
Calling Identity Features 3-49
Calling Identity Delivery 3-49
Calling Line Identification Presentation (CLIP) 3-50
Calling Identity Delivery Blocking (CIDB) 3-51
Calling Line Identification Restriction (CLIR) 3-54
Direct Inward/Outward Dialing for PBX 3-58
Analog DID for PBX 3-58
DOD For PBX 3-59
Seasonal Suspend 3-59
Seasonal Suspend Feature for Release 5.0 MR1 and Earlier 3-59
Seasonal Suspend Feature for Release 5.0 MR1.1 and Later 3-63
Terminal and Group Make Busy Services 3-66
Feature Interactions 3-67
Configuring 3-68
Features for Centrex Subscribers Only 3-68
Call Hold (CHD) 3-69
Call Park and Call Retrieve 3-71
Direct Inward/Outward Dialing for Centrex 3-71
Directed Call Pickup (With and Without Barge-In) 3-72
Distinctive Alerting/Call Waiting Indication (DA/CWI) 3-73
Additional Features Applicable to Centrex and POTS 3-73
Anonymous Call Rejection (ACR) 3-74
Automatic Callback (AC)—Repeat Dialing 3-75
Automatic Recall (AR)—Call Return 3-76
Call Block - Reject Caller (CBLK) 3-78
Call Transfer (CT) 3-79
Change Number (CN) 3-80
Customer-Originated Trace (COT) 3-80
Do Not Disturb (DND) 3-81
Hotline Service 3-81
Hotline-Variable Service (HOTV) 3-82

Interactive Voice Response (IVR) Functions 3-85
Limited Call Duration Service (Prepaid/Postpaid) with RADIUS Interface to AAA 3-86
Message Waiting Indicator (MWI)—Audible and Visual 3-89
Multiline Hunt Group (MLHG) 3-90
Multiline Variety Package 3-105
Multiple Directory Numbers (MDN) 3-106
No Solicitation Announcement (NSA) 3-106
Own Calling Number Announcement (OCNA) 3-111
Privacy Screening (Calling Identity with Enhanced Screening) 3-111
Speed Call 3-115
Subscriber-Controlled Services and Screening List Editing (SLE) 3-116
Temporarily Disconnected Subscriber Status and Soft Dial Tone 3-119
Three-Way Calling (TWC) 3-121
Three-Way Calling Deluxe (TWCD) 3-122
Usage-Sensitive Three-Way Calling (USTWC) 3-127
Visual Message Waiting Indicator (VMWI) 3-127
Voice Mail (VM) and Voice Mail Always (VMA) 3-127
Warmline Service 3-134
Office Service ID and Default Office Service ID 3-134
Notes on Bundling Features in Services 3-135

CHAPTER 4

Class of Service Restrictions and Outgoing Call Barring Features 4-1

Class of Service Restrictions 4-1
How to Use This Section of the Document 4-2
COS Functional Description 4-2
Exemptions from COS and OCB Restrictions 4-2
National Call Restrictions (Toll Restrictions) 4-3
Overview—Black and White List Features 4-3
Casual Call (101XXXX) White and Black Lists (Number Blocking) 4-4
National White and Black Lists (Number Blocking) 4-4
International White and Black Lists (Number Blocking) 4-5
Originating Line Information White and Black Lists 4-5
Nature of Dial White and Black Lists 4-6
Blocking Flags 4-6
Account Codes and Authorization Codes 4-7
ANI Screening on Incoming Calls 4-10
Temporary Disconnect Treatment 4-10
COS Restriction Priorities 4-11

High-Level Flowchart of COS Screening Process 4-11
Outgoing Call Barring (OCB) 4-14
OCB Highlights 4-15
OCB Subscription and Provisioning 4-15
OCB Activation and User Options 4-16
OCB Deactivation 4-17
OCB Interrogation 4-17
OCB Invocation and Screening 4-18
OCB Lockout Behavior 4-18
How to Coordinate OCB and COS Provisioning 4-18
OCB Feature Interactions 4-20
Limitations and Restrictions 4-20
Additional Documents with OCB Information 4-21

CHAPTER 5 **Feature Interactions** 5-1
Overview of Features and Services 5-2
Creation of Features and Services 5-2
Trigger Detection Points, Trigger IDs, and Call States 5-5
Feature Precedence 5-7
Feature Inhibition 5-9
Special Interaction Scenarios 5-13
DND and CFB Interaction 5-13
CHD, CFNA, and CW Interaction for Centrex Subscriber 5-13
Examples of Interactions 5-14
Three-Way Call Interaction 5-14
Call Waiting Interaction 5-15
Calling Number Delivery Interaction 5-15

CHAPTER 6 **Interactive Voice Response Functions** 6-1
RACF 6-2
Using IVR Functions for RACF 6-2
RACF PIN Change 6-5
Screening-List-Editing Services 6-7
Using IVR for Selective Call Forwarding 6-7
Using IVR for SCA, SCR, and DR/CW Services 6-15
Two-Level Automatic Recall Activation 6-22
No Solicitation Announcement 6-24
NSA Activation 6-25

Privacy Screening 6-38
Subscriber Activation and Management of Privacy Screening 6-39
Caller Interaction with Privacy Screening 6-40
Subscriber Interaction with Privacy Screening 6-42
Multi-Lingual Support Feature 6-45
MLS with ThinkEngine Networks or IPUnity 6-47
MLS with IOS 6-48
MLS Feature Interactions 6-48
MLS Announcements 6-48
MLS Provisioning 6-49

INDEX

Preface

Revised: March 24, 2011, OL-12606-21

This document describes the network features and subscriber features supported by the Cisco BTS 10200 Softswitch. It explains the behavior of each feature from the end-user perspective, and the effect of provisionable options on feature behavior. This document is designed for engineers, technicians, and system administrators who install, configure, and operate the BTS 10200.

Caution Some features involve the use of other network elements (NEs) deployed in the service provider network, for example, gateways, media servers, announcement servers, eMTAs, and SIP phones. See the Component Interoperability section of the *Release Notes* for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the BTS 10200 Release 5.0 software. Earlier or later releases of platform software might be interoperable and it might be possible to use other functions on these platforms. The list in the *Release Notes* certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the BTS 10200.

Conventions

This document uses the following conventions:

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

Caution Means *reader be careful.* In this situation, you might do something that could result in equipment damage or loss of data.

Updates to this Document for Release 5.0

Version OL-12606-21

Updated the "Group Speed Call" section on page 3-116 and "Treatment of Outbound Call Features" section on page 3-95.

Version OL-12606-20

The following information was added in version OL-12606-20:

- Added the subscriber details for which the Customer Originated Trace (COT) feature is inhibited. See "Customer-Originated Trace (COT)" section on page 3-80 for details.
- Updated the "Provisionable Parameters for VM and VMA" section on page 3-130.
- Enhanced the "Call Transfer (CT)" section on page 3-79.

Version OL-12606-19

Updated the "Change Number (CN)" section on page 3-80 to include additional descriptive information.

Version OL-12606-18

The following information was added in version OL-12606-18:

- Added the description for Change Number feature. See "Change Number (CN)" section on page 3-80.

Version OL-12606-17

The following information was added in version OL-12606-17:

- Information regarding the block all inbound calls feature. See "Block All Inbound Calls" section on page 3-79.
- Information regarding the provisioning of ANI screening on incoming calls. See "ANI Screening on Incoming Calls" section on page 4-10.

Version OL-12606-16

The following information was changed in version OL-12606-16:

- Information was corrected in the "Option to Send Redirecting Number as CPN for Redirected Calls" section on page 1-20.

Version OL-12606-15

The following information was changed in version OL-12606-15:

- Information was corrected in the notes for Figure 3-4, "Searching an MLHG—Incoming Call to an Individual Terminal (Example)".

Version OL-12606-14

Information regarding the interaction between the AR feature and CFB feature was added. See "CFB Feature Interactions" section on page 22.

Version OL-12606-13

Information was added regarding the following features:

- The ENUM capability feature. See the "ENUM Capability" section on page 47.
- The Multiline Variety Package feature. See the "Multiline Variety Package" section on page 105.
- The Seasonal Suspend feature. See the "Seasonal Suspend Feature for Release 5.0 MR1 and Earlier" section on page 60 and "Seasonal Suspend Feature for Release 5.0 MR1.1 and Later" section on page 63.
- Terminal and Group Make Busy Services. See the "Terminal and Group Make Busy Services" section on page 66.
- The CMTS Discovery Using Static Subnet Table feature. See the "CMTS Discovery Using the Static Subnet Table" section on page 46
- The Aggregation Id Subnet feature. See the "Aggregation Id Subnet" section on page 47.

Version OL-12606-12

Updated the information for Temporarily Disconnected Subscriber Status and Soft Dial Tone. See the "Temporarily Disconnected Subscriber Status and Soft Dial Tone" section on page 3-119.

Updated the Split-NPA information with a limitation note. See the "Split-NPA" section on page 1-38.

Version OL-12606-11

Information was added regarding protocol interworking for T.38 fax. See the "Protocol Interworking" section on page 1-43.

Additional details were added regarding the treatment of timeout and application server parameters for the voice-mail feature. See the "Provisionable Parameters for VM and VMA" section on page 3-130.

Version OL-12606-10

References to music on hold were removed for the Call Park and Privacy Screening features. The music on hold is not a feature provided by the BTS 10200 (although music can be provided by some third-party servers). Changes were made in Chapter 3, "Subscriber Features."

Version OL-12606-09

Information was added regarding the treatment of incoming calls when certain subscriber features are invoked. See the "Multiline Hunt Group (MLHG)" section on page 3-90.

The MDN feature description was updated to include multiple secondary numbers. See the "Multiple Directory Numbers (MDN)" section on page 3-106

The new OCNA feature was added. See the "Own Calling Number Announcement (OCNA)" section on page 3-110

Additional details about account code and authorization code provisioning options was added in the "Account Codes and Authorization Codes" section on page 4-7.

Version OL-12606-08

A reference list of announcements was added at the end of the Privacy Screening description in the "Privacy Screening" section on page 6-38.

Version OL-12606-07

Information about the interaction of CHD, CW, and CFNA was changed for Release 5.0, Maintenance Release 1.1. See the "Call Hold (CHD)" section on page 3-69.

Version OL-12606-06

Information about MLHG features and feature activation was added in the "Multiline Hunt Group (MLHG)" section on page 3-90.

Additional information about call types was added in the "National White and Black Lists (Number Blocking)" section on page 4-4.

Cross references to CLI commands were updated to provide a link to the *Cisco BTS 10200 Softswitch CLI Database*. Other cross references were updated as needed.

Version OL-12606-05

All lawful intercept and CALEA information was moved to a new chapter, Chapter 2, "Lawful Intercept and Enhanced CALEA Features," and information was updated as needed for this release.

For Release 5.0, Maintenance Release 1, and later, terminating SIP triggers were added for SIP subscribers. See the "SIP Triggers" section on page 1-27. In addition, several updates and clarifications were added in this section.

The "Outgoing Call Barring (OCB)" section on page 4-14 was reorganized for ease of use; information from all earlier software releases was combined into a single complete description of the feature.

Throughout the document, references to the Cognitronics brand name were updated to ThinkEngine Networks.

Version OL-12606-04

Clarifying examples were added to help explain the interaction of CHD, CW, and CFNA. See the "Call Hold (CHD)" section on page 3-69. A cross reference to this information was also added in the "CHD, CFNA, and CW Interaction for Centrex Subscriber" section on page 5-13.

Clarification was added that the reminder ring option is not provided for SIP endpoints. See the "Do Not Disturb (DND)" section on page 3-81.

For Release 5.0, Maintenance Release 1, and later, provisionable parameters are added for collection of account codes for certain call types and endpoints. See the "Account Codes (Nonverified) Tone-Based Operation" section on page 4-7.

Version OL-12606-03

The reference specification for lawful intercept was updated to PKT-SP-EM1.5-I02-050812 in Chapter 2, "Lawful Intercept and Enhanced CALEA Features."

A reference to supported call types was added to the "National White and Black Lists (Number Blocking)" section on page 4-4.

Editorial clarifications were made in the "SIP Triggers" section on page 1-27.

Version OL-12606-02

Additional clarifications were added regarding MLHG in Multiline Hunt Group (MLHG), page 90.

REFER and REPLACES features were added to the list of valid features in the "Office Service ID and Default Office Service ID" section on page 3-134. Additional editorial clarifications were also made in this section.

Information about the black/white lists was clarified in the "Overview—Black and White List Features" section on page 4-3.

Version OL-12606-01

This document includes all of the information about telephony features that was contained in the previous issue (Release 4.5.x) of the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions*, and has been updated to incorporate Release 5.0 features. These include:

- Chapter 1, "Network Features"
  - "8XX (Toll-Free Calling)" section on page 1-13
  - "911 Overflow Announcement" section on page 1-10
  - "Emergency 911 Trunk Connection Loss Alarm" section on page 1-10
  - "SIP Triggers" section on page 1-27
  - "RFC 2833 DTMF Relay—Call Agent Controlled Mode" section on page 1-24
  - "Network Loopback Test for ISDN PRI Trunks" section on page 1-61
  - Minor updates and corrections in the following sections: "Active Call Information Display" section on page 1-16, "Alerting Notification to Third-Party Feature Server" section on page 1-17, "Calling Party Number Options for Outbound SETUP Messages" section on page 20, and "T.38 Fax Relay, Modem, and TDD Handling" section on page 1-38.
- Chapter 2, "Lawful Intercept and Enhanced CALEA Features"—New chapter added July, 2007 to collect all information on this topic.
- Chapter 3, "Subscriber Features"
  - Added a note in the "Call Forwarding Features" section on page 3-6 referring to information about the SIP call redirection (302) feature.
  - Added a note to clarify the behavior of the AC and AR features when there is a FS switchover. See "Automatic Callback (AC)—Repeat Dialing" section on page 3-75 and Automatic Recall (AR)—Call Return, page 3-76.
  - Added information on MWI reset through CLI commands. See "Message Waiting Indicator (MWI)—Audible and Visual" section on page 3-89.
  - Added information to the "Multiline Hunt Group (MLHG)" section on page 3-90.
  - Added information to the "Privacy Screening (Calling Identity with Enhanced Screening)" section on page 3-111.
  - Clarified the interaction between the OFFICE-SERVICE-ID and DEFAULT-OFFICE-SERVICE-ID parameters. See Office Service ID and Default Office Service ID, page 3-134.
- Chapter 4, "Class of Service Restrictions and Outgoing Call Barring Features"—(none)
- Chapter 5, "Feature Interactions"—(none)
- Chapter 6, "Interactive Voice Response Functions"—Added the "Privacy Screening" section on page 6-38 and the "Multi-Lingual Support Feature" section on page 45.

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

CHAPTER 1

Network Features

Revised: March 24, 2011, OL-12606-21 (Release 5.0)

The Cisco BTS 10200 Softswitch supports network features as described in the following sections:

- Interoperability
- Numbering Plans and Dialing Procedures—This section includes information on digit manipulation, E.164 dialing plan, casual dialing (dial around), dial 1 options, directory services, easily recognizable codes, Information service calls (900 and 976), n11 support (211, 311, 411, 511, 611, 711, 811). and NRUF reporting.
- Emergency Services (911)
- Operator Services—This section includes information on Busy Line Verification and Operator Interrupt.
- Network Services—This section includes information on 8XX (Toll-Free Calling), Active Call Information Display, Alerting Notification to Third-Party Feature Server, Calling Party Number Options for Outgoing SETUP Messages, Dialing Parity (IntraLATA Toll Presubscription), Local Number Portability (LNP), SIP Triggers, Split-NPA, and T.38 Fax Relay.
- Trunk and Line Testing

In general, BTS 10200 features delivered via gateway clients behave identically to their public switched telephone network (PSTN) counterparts.

Note For information on subscriber features, see Chapter 3, "Subscriber Features." For information on outgoing call restriction options (Class of Service and Outgoing Call Barring) see Chapter 4, "Class of Service Restrictions and Outgoing Call Barring Features."

Some features can be accessed and controlled by the subscriber using a handset and vertical service codes (VSCs). VSCs are provisionable by the service provider (any valid unique ASCII string up to five characters long), and the customary values are country specific. The VSC values used throughout this chapter are for illustration purposes. For convenience, some VSC values are preprovisioned in the BTS 10200. The valid formats for VSC ASCII strings are listed in the Vertical Service Code commands in the *Cisco BTS 10200 Softswitch CLI Database*. To view the current VSC values provisioned on your system, use the **show vsc** CLI command. To provision VSCs, see the VSC provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Typically, the system responds to user handset actions by providing an appropriate announcement. However, if an announcement is not provisioned or cannot be played, an alternate tone (for example, reorder tone) is played. Announcements are listed in the *Cisco BTS 10200 Softswitch Provisioning Guide*, and tones are listed in the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

Interoperability

The BTS 10200 interworks with a wide range of network elements (NEs), but there are certain limitations. Cisco recommends that you keep the following caution in mind as you prepare to purchase and use NEs for your network.

Caution Some features involve the use of other NEs deployed in the service provider network, for example, gateways and media servers. See the Component Interoperability section of the *Release Notes* for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the BTS 10200 Release 5.0 software. Earlier or later releases of platform software might be interoperable and it might be possible to use other functions on these platforms. The list in the *Release Notes* certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the BTS 10200.

Numbering Plans and Dialing Procedures

The BTS 10200 supports the numbering plans and dialing procedures listed in Table 1-1. These features are described in the sections that follow.

Note For additional details on the rules used in the numbering plans and dialing procedures, see the *Cisco BTS 10200 Softswitch Dial Plan Guide*.

Table 1-1 Support for Numbering Plans and Dialing Procedures

Feature Description	Reference
Digit Manipulation	
E.164 Dialing Plan Implementation	ITU-T Recommendation E.164
Casual Dialing (Dial Around)	
Dial 1 Options for Local, Toll, and InterLATA Calls	
Directory Services (411, 555-1212, 0+ Listing Services)	GR-532-CORE FSD-30-17-0000
Easily Recognizable Codes	GR-2892-CORE SR-2275, Sec. 3.3
Information Service Calls (900 and 976)	
n11 support (211, 311, 411, 511, 611, 711, 811)	GR-532-CORE FSD-30-16-0000
NRUF Reporting for NANPA Audit Support	

Digit Manipulation

The Digit Manipulation (DIGMAN) feature provides the ability to modify both calling number and called number for both incoming and outgoing calls within the BTS 10200.

The calling party number is also known as ANI (automatic number identification). The called party number is also known as DNIS (dialed number identification service).

In addition to modifying the calling number and the called number, the digit manipulation tables can be used to modify the nature of address (NOA) of ANI and/or DNIS numbers. This feature provides the following benefits in the service provider network:

- Dial plans for both North American Numbering Plan (NANP) and ITU-T E.164 numbering plan
- Flexible call processing
- ANI- or DNIS-based routing

For additional standards information, see the following industry sources:

- NANP—See http://www.nanpa.com
- ITU-T Recommendation E.164, *The International Public Telecommunication Numbering Plan*

The BTS 10200 performs digit manipulation by matching and replacing digits in the digit string that is being processed.

E.164 Dialing Plan Implementation

The BTS 10200 implements a dialing plan based on ITU-T Recommendation E.164, *The International Public Telecommunication Numbering Plan*, a standard for numbering and routing. This dialing plan uses a generic numbering scheme for number evaluation. The BTS 10200 performs digit manipulation on ANI data of the calling party, and on DNIS data of the called party.

National Number

In the E.164 numbering scheme, there are three parts to any national number (number that terminates within the country):

- National destination code (NDC)—A region of the country (1 to 6 digits, typically 3). Provisioning of the NDC is optional. Some countries do not use NDCs in the national number.
- Exchange code (EC)—An area served by a single central office (CO) switching facility (1 to 6 digits, typically 4).
- Dialing number (DN)—The specific digits that identify a subscriber line (1 to 4 digits, typically 4).

The combination [EC + DN] is called the subscriber number (SN).
The combination [NDC + EC + DN], or [NDC + SN], is called the national number (NN).

[NDC + EC + DN] is interpreted as [NPA + NXX + XXXX] in NANP, where NPA (numbering plan area) = 200 to 999, NXX (office code) = 200 to 999, and XXXX = 0000 to 9999. The BTS 10200 applies the NANP interpretation if the NANP-DIAL-PLAN flag is set to Y (yes) in the DIAL-PLAN-PROFILE table.

A user originates a call by dialing as follows:

- To place a call to a phone in the same EC (served by the same CO), dial the SN. In most cases, this is considered a local call.

- To place a call to a phone in another EC, but within the same region (same NDC), dial the SN. In most cases, this is considered a local toll call.
- To place a call to a phone in another region (different NDC), dial the national (trunk) prefix and the NN. The national prefix varies from country to country. In most cases, this type of call is considered a national toll call.

  Examples of national prefixes include:

  - 0 in China
  - 1 and 0 within NANP
  - 9 in Finland and Spain
  - 16 in France

For countries that do not use NDCs, it is not necessary to provision any value for the NDC parameter in the BTS 10200.

International Number

The international number is the number dialed from one country to another to reach a subscriber. Each country is assigned a country code (CC). The international number is the combination [CC + NN], or [CC + NCD + EC + DN]. Table 1-2 lists several examples.

Table 1-2 Examples of International Numbers

Country	City	CC	NDC	EC	DN Group	Complete International Number
Belgium	Bruxelles	32	02	123	xxxx	32-02-123-xxxx
China	Chengdu	86	28	8293	xxxx	86-28-8293-xxxx
Germany	Dusseldorf	49	211	12	xxxx	49-211-12-xxxx
Canada	Montreal	1	514	870	xxxx	1-514-870-xxxx
United Kingdom	London	44	71	248	xxxx	44-71-248-xxxx

To place a call to a phone in another country, the caller must dial an international prefix and then the international number. Thus, the complete digit string to dial is [international prefix + CC + NN]. The international prefix varies from country to country. Examples of international prefixes include:

- 00 in China

  Example of a call from China to Montreal: 00-1-514-870-xxxx
- 011, 01 in NANP

  Example of a call from the United States to Bruxelles: 011-32-02-123-xxxx

In some countries, two or more international prefixes may be used

- To reach different groups of countries
- To reach countries within a group

Casual Dialing (Dial Around)

Casual dialing, also known as dial around, specifies whether the carrier supports 101XXXX calls. The digit map CLI command tokens provide the digit pattern. The digit pattern specifies all possible acceptable patterns. An example of a casual digit pattern is 1010321 or 1010220. The digit map table tells the media gateway (MGW) how to collect and report dialed digits to the Call Agent (CA). Subscribers can prefix their toll, interLATA, or international calls with 101XXXX. Casual dialing supports the following casual calls:

- 101XXXX + 0/1 + NPA + NXX-XXXX
- 101XXXX + 0/00
- 101XXXX + 011/01 + CC + NN

Dial 1 Options for Local, Toll, and InterLATA Calls

The service provider can provision the system to control the use of prefix 1 for specific types of calls and for specific subscribers. Local, toll, and interLATA call types can each be independently provisioned in the subscriber-profile table as follows:

- Require that the number be dialed with a prefix 1—If the system is provisioned this way, and the caller attempts to dial the number without using a prefix 1, the system rejects the call and provides an appropriate announcement (Release Code 10).
- Require that the number be dialed without a prefix 1—If the system is provisioned this way, and the caller attempts to dial the number using a prefix 1, the system rejects the call and provides an appropriate announcement (Release Code 9).
- Prefix 1 optional—Allow call processing to proceed whether a prefix 1 is dialed on not.

For service access code (SAC) calls such as 500, 700, 800, and 900, the user must dial the prefix 1. The flags LOCAL-PFX1-OPT, INTERLATA-PFX1-OPT, and TOLL-PFX1-OPT in the Subscriber table do not affect these types of calls.

For a list of the specific provisioning parameters, see the Subscriber Profile table in the *Cisco BTS 10200 Softswitch CLI Guide*. For a complete list of release cause codes, see the Appendix of the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Directory Services (411, 555-1212, 0+ Listing Services)

The BTS 10200 supports the directory services access feature as specified in Telcordia document GR-352-CORE, LSSGR: *Interface To Directory Assistance Systems (FSD 30-17-0000)*.

Directory services allows a subscriber to obtain the listed telephone number for a given name and address. The caller dials a specific service number to reach directory services, also referred to as directory assistance (DA). When a subscriber dials one of the following digit patterns, the BTS 10200 routes the call to the applicable directory services in the PSTN:

- 411 or 555-1212 (DA)
- 1+411, 1+555-1212 (toll DA)
- 1-NPA-555-1212 (mostly for out-of-town/state numbers)
- 1-8XX-555-1212 (toll-free numbers)
- 0+ listing services

The service to the caller can be provided manually by a live operator, automated via a voice or dual tone multifrequency (DTMF) recognition system, or by a combination of these. The volume level from an automated voice-response unit, however, should be comparable to that of a live operator. Different network operators can employ different systems in providing directory services.

A typical directory services request requires that the caller first give the name of the town and city. The caller then provides the name of the person or business that the caller wants to call, including the spelling of unusual names. Finally, the caller states if the request is for residence or business. Additional services include handling multiple requests made during the same call and automatic connection to the person (or business) the caller wants to call.

Easily Recognizable Codes

The BTS 10200 supports selected easily recognizable codes (ERCs) as described in document SR-2275, *Telcordia Notes On the Network*, Section 3.3. The supported ERCs are

- 500 personal communications services (PCS)—See the Alliance for Telecommunications Industry Solutions (ATIS) document INC-95-0407-009, *Personal Communication Services N00NXX. Code Assignment Guidelines*, for a PCS description.
- 700 service access calls (SAC)—Range of codes used by interexchange carriers (IXCs) to provide services on the network.
- Toll-free service call features (8XX)—See the "8XX (Toll-Free Calling)" section on page 1-13 for a description.
- 900/976 information service calls—See the "Information Service Calls (900 and 976)" section on page 1-6 for a description.

Other Telcordia reference documents include:

- SR-2275, *Telcordia Notes On the Network*
- GR-2892-CORE, *Switching and Signaling Generic Requirements for Toll-Free Service Using AIN*

Information Service Calls (900 and 976)

Information service calls (ISCs) provide a variety of announcement-related services on a national or local basis. There are two general categories of this service:

- Public announcement services (PAS)—Weather, sports, horoscope, and so forth
- Media-stimulated calling (MSC)—Telephone voting, radio station call-ins, and so forth

National calls are dialed as 1-900-xxx-xxxx and local calls are dialed as NPA-976-xxxx.

n11 support (211, 311, 411, 511, 611, 711, 811)

Note 911 service is covered in the "Emergency Services (911)" section on page 1-8.

This section describes BTS 10200 support for n11 services. The typical relationship between the n11 codes and the nature of dial (NOD) values is as follows.

n11 Code	NOD Value
211	INFO
311	NON-EMG
411	DA
511	TRAFFIC
611	REPAIR
711	RELAY
811	BUSINESS

For a complete list of NOD values, see the Nature of Dial command in the *Cisco BTS 10200 Softswitch CLI Database*. To view the current NOD values provisioned on your system, use the **show nod** CLI command.

For additional information on n11 calling, see the following industry documents:

- Telcordia document GR-352-CORE, *LSSGR: Service Codes N11 (FSD 30-16-000)*
- The NANPA web site, http://www.nanpa.com/number_resource_info

Community Information and Referral Services (211)

The 211 service provides access to information from government service agencies and certain public charity groups.

Nonemergency Services (311)

Some city governments offer 311 service to provide nonemergency information to the community. The caller dials 311 and the Call Agent translates this to the closest nonemergency access office.

The BTS 10200 supports nonemergency services (311) for routing calls to a specified route type and identification. Routes for all nonemergencies (311) are allocated through the destination table by defining the call type (call-type=NON-EMG) and the routing information for the dialed digits.

Directory Assistance (411)

The 411 service provides directory assistance. See the "Directory Services (411, 555-1212, 0+ Listing Services)" section on page 1-5.

Traffic and Transportation Information (511)

The 511 service provides access to information about local traffic conditions.

Repair Service (611)

The 611 service connects to the local telephone repair service (if the service provider offers this service).

Telecommunications Relay Services (711)

The 711 service provides access to telecommunications relay services (TRS).

Local Billing Services (811)

The 811 service connects to the local telephone billing office.

NRUF Reporting for NANPA Audit Support

Numbering Resource Utilization and Forecast (NRUF) reporting provides NANPA audit data based on provisioned values in the dn2subscriber table. For FCC-required NANPA audit compliance, the report input is NPANXX. In markets outside of NANPA, the input can be based on either the combination of the NDC and the EC, or just the EC.

The data for NRUF reporting is generated based on either the NDC or the EC. The service provider can use the **report dn-summary** command to generate the following reports:

- Report on all DNs belonging to a specific NDC and EC.
- Report on a thousands group within a specific NDC and EC.

For additional details of this feature, see the NRUF chapter of the *Command Line Interface Reference Guide*.

Emergency Services (911)

The BTS 10200 supports emergency services (911) as specified in Telcordia document GR-529-CORE, *LSSGR: Basic 911 Emergency Service (FSD 15-01-0000)*.

Other Telcordia reference documents include

- SR-4163, *E9-1-1 Service Description*
- GR-350-CORE, *E911 Public Safety Answering Point: Interface Between a 1/1A ESS Switch and Customer Premises Equipment*

This section covers the following topics:

- "Description" section on page 1-8
- "Important Provisioning Requirements" section on page 1-9
- "911 Overflow Announcement" section on page 1-10
- "Emergency 911 Trunk Connection Loss Alarm" section on page 1-10
- "Feature Interactions" section on page 1-10
- "Feature Provisioning Commands" section on page 1-10

Description

The digit string 911 is typically used in the U.S. Other digit strings are used elsewhere in the world.

Emergency service is a public safety feature providing emergency call routing to a designated Emergency Service Bureau (ESB), normally called the public safety answering point (PSAP) in the United States. The 3-digit 911 number is assigned for public use in many areas of the United States and Canada for reporting an emergency and requesting emergency assistance. Depending on municipal requirements and procedures, an ESB attendant can transfer the call to the proper agency, collect and relay emergency information to the agency, or dispatch emergency aid directly for one or more participating agencies.

911 calls are location dependent and must be selectively routed to the appropriate PSAP depending on where the call originates. The routing process is part of the Enhanced 911 (E911) feature set and works as follows:

1. In the PSTN, the local serving end office routes the call to the designated E911 tandem for that serving area.
2. The E911 tandem then routes the call to the proper PSAP.

Once the caller is connected to the PSAP attendant, the PSAP system typically displays the caller's directory number to the PSAP attendant. Additional data (such as the subscriber's name, address and closest emergency response units) may also be retrieved from the local carrier automatic location identification (ALI) database and displayed to the PSAP attendant.

The service provider can provision a flag for each subscriber to specify which number to send with emergency calls—the subscriber directory number or the subscriber billing number.

Special emergency functions can be provided via a channel-associated signaling (CAS) trunking gateway (TGW) that supports ESB trunks or emergency service line (ESL) trunks with MF signaling. Examples of special emergency functions include:

- Operator callback—Allows the PSAP to automatically ring back the caller.
- End-to-end called-party hold—The BTS 10200 keeps the connection active even if the caller goes on hook.
- Operator disconnect—Allows the PSAP to terminate the call even though the caller has not gone on hook.

Important Provisioning Requirements

For service providers in the U.S., it is typical to provision the Destination table with call-type=EMG for the digit string 911, and call-subtype=NONE (default), because 911 is a central dispatch point for all emergency, ambulance, fire, and police calls.

Caution On the BTS 10200, for a call to be considered an emergency, it must be provisioned as call-type EMG. If you are using separate DNs for ambulance, fire, and police service (typically applies to networks outside the U.S.), Cisco strongly recommends that you provision these as call-type EMG and call-subtype <AMBULANCE or FIRE or POLICE> in the Destination table. This is the only way to be sure that they will be given all the treatment of the EMG call-type.

Depending on the region of the world, the provisionable timers may require different values, or may not be needed, and they can be turned off. The called-party control feature, typically used in the United States, can also be turned off. All other functions of the emergency number are the same as for the 911 feature.

The emergency service feature can be made available to all subscriber lines connected to a BTS 10200 using the default office service ID, or to all subscribers in a specific POP using the office service ID. See the "Office Service ID and Default Office Service ID" section on page 3-134 for a general description of this provisionable service.

911 Overflow Announcement

The system plays an announcement when all circuits to the emergency center are busy and the emergency call cannot be completed to the emergency center. An example of an announcement for this feature is, "We are experiencing 911 difficulties. Please hang up and dial 0 to reach an operator for emergency assistance." The announcement is applied when the announcement resource is available and applicable. For the specific cause code and announcement ID, see "Appendix A, Cause Code to Announcement ID Mappings" in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Emergency 911 Trunk Connection Loss Alarm

The BTS 10200 is capable of generating a critical alarm of when an emergency trunk resource becomes remotely or locally blocked. This alarm will be raised when any of the following events occurs:

- The gateway becomes unreachable.
- The emergency trunk termination is administratively made OOS through CLI commands on the BTS 10200.
- The emergency trunk termination is remotely or locally blocked.

This feature is applicable only to emergency trunks of type CAS, SS7 and ISDN. The EMERGENCY-TRUNK-GROUP token in the applicable trunk group table must be provisioned to support this feature. For CAS trunk groups, the E911 / EMERGENCY-TRUNK token must also be provisioned.

Feature Interactions

The following feature interactions apply to emergency calls (call-type=EMG):

- During a 911 call from a subscriber line, the call waiting (CW) and three-way calling (TWC) features are automatically disabled for the subscriber line.
- There is an interaction when a Centrex subscriber invokes call hold (CHD) and places a call to an emergency number:
  - When the emergency operator answers the call, a two-party call is active between the subscriber and the emergency operator. The on-hold party remains on hold.
  - When the subscriber presses the Flash button or hookswitch, a three-way call is established among the subscriber, the emergency operator, and the previously on-hold party.
  - It is not possible to place the emergency operator on hold.

Feature Provisioning Commands

To provision this feature, see the 911 provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Operator Services

The BTS 10200 supports operator services as specified in Telcordia Requirement FR-271, *Operator Services Systems Generic Requirements (OSSGR)*.

Operator services is a call-processing function whereby callers can access either a live operator or an automated function to complete calls or gain access to information. The service provider can provide this feature or outsource it to a third-party vendor. Some additional functions accomplished by operator services include automatic call distribution, billing detail recording, and information retrieval.

This section includes the following additional topics:

- Numbers Used to Access Operator Services, page 1-11
- Types of Services, page 1-11
- Busy Line Verification (BLV) and Operator Interrupt (OI) Services, page 1-12

Numbers Used to Access Operator Services

The following numbers are commonly used to access operator services:

- 0—Local operator support
- 00—Operator support outside the “local” calling area, using a presubscribed interexchange carrier (PIC)
- 0+ area code and number—Operator support when the destination number is known (that is, for collect calls, calling card calls, person-to-person calls, and so forth, using PIC
- CAC+0+—Operator services, using a dialed carrier access code (CAC)
- 01+CC+NN—International operator services, using PIC
- CAC+01+CC+NN—International operator services, using a dialed CAC

Types of Services

Operator services provided to callers typically include:

- Assistance
- General information
- Directory assistance
- Dialing instructions
- Rate information
- Credit recording
- Trouble reporting
- Call completion
- Alternate billing services (ABS)
- Calling card calls
- Collect calls
- Third-number calls

- Handling options
- Person-to-person
- Conference calls
- Call transfer
- Real-time rating
- Rate quotes
- Time and charges
- Notify

Busy Line Verification (BLV) and Operator Interrupt (OI) Services

This section describes busy line verification (BLV) and operator interrupt (OI) services. OI is also referred to as emergency interrupt (EI). BLV and OI services are based on GR-1176 (FSD 80-01-0300), *Busy Line Verification*, part of Telcordia OSSGR requirements (FR-271).

Description and Operation

BLV service permits the user to obtain operator assistance to determine if a called line is in use. The user dials 0, waits for the operator to pick up the line, and requests BLV service. OI service permits the operator to speak directly with the busy party. The service provider can deny BLV service to any subscriber by setting type=denied for fname=BLV in the subscriber-feature-data table (see the BLV provisioning link listed below). Note that denying BLV also denies OI.

BLV and OI services work as follows:

1. The user calls the operator and requests BLV service regarding a specific called line.
2. The operator provides the BLV service.
3. For OI, the operator interrupts the conversation in progress and relays a message.
4. If the interrupted party at the called line is willing to hang up, they do so.
5. The user can originate a new call to the called DN.

Note At the user's request, the operator has the option to directly connect the user to the called line.

The BLV feature can be made available to all subscribers lines connected to a BTS 10200 using the default office service ID, or to all subscribers in a specific POP using the office service ID. See the "Office Service ID and Default Office Service ID" section on page 3-134 for a general description of this provisionable service.

Feature Interactions

The following feature interactions are applicable to the BLV and OI services:

- When the operator attempts BLV, if the verified party is engaged in a call and has features currently invoked, the operator might receive a busy tone and might not be able to perform an interrupt on the call. In this section, "currently invoked" means that another feature has already been triggered in the

call. There are a few exceptions, such as Cancel Call Waiting (CCW) and Do Not Disturb (DND); for example, BLV can be successfully performed even if CCW or DND is currently invoked on the call.

- If the verified party (terminating subscriber) has call forwarding unconditional (CFU) activated, the operator will receive a busy tone and will not be able to perform an interrupt on the call.

Feature Provisioning Commands

To provision this feature, see the BLV provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Network Services

The BTS 10200 supports the network services listed in Table 1-3.

Table 1-3 Support for Network Services

Feature Description	Reference
8XX (Toll-Free Calling)	SR-2275, Sec. 14.6
Active Call Information Display	
Alerting Notification to Third-Party Feature Server	
Calling Party Number Options for Outbound SETUP Messages	
Dialing Parity (IntraLATA Toll Presubscription)	FSD-20-24-0040 TR-TSY-000693
Local Number Portability (LNP)	ATIS/T1S1 T1.TRQ-02-2001
RFC 2833 DTMF Relay—Call Agent Controlled Mode	Section 7.1.1 of PKT-SP-NCS1.5-I01-050128 Section 7.1.1 of PKT-SP-TGCP1.5-I01-050128
SIP Triggers	
Split-NPA	INC97-0404-016
T.38 Fax Relay, Modem, and TDD Handling	IETF RFC 2833 ITU-T *Recommendation T.38*
ENUM Capability	

8XX (Toll-Free Calling)

The purpose of the toll-free feature is to have the called party, rather than the calling party, charged for the call. These calls are prefixed with the 1+8XX service access codes. The seven digits following the 8XX codes are used for routing the call. For an inbound/outbound 8XX call, the BTS 10200 checks the local toll-free database first. If the corresponding DN is not found in the local toll-free database, the system sends a query to the service control point (SCP) to request the corresponding DN.

All aspects of toll-free calling are transparent to the caller. A caller expects to dial 1-8XX-NXX-XXXX to reach the desired destination. The company that translates the number to a specific DN, and the company that routes the call, must appear transparent to callers. Most callers are not aware that their dialed 8XX number is changed into a specific DN. What matters to the callers is that they reach what they perceive to be the called number, and they are not billed for the call.

Note These toll-free (8XX) features can be made available to all subscriber lines connected to a BTS 10200 using the default office service ID, or to all subscribers in a specific POP using the office service ID. See the "Office Service ID and Default Office Service ID" section on page 3-134 for a general description of this provisionable service.

8XX Call Processing

The system processes outbound 8XX calls as follows:

1. The CA signals the AIN FS to perform an 8XX query.
2. The AIN FS performs an internal database query.
3. If an internal record is found for the 8XX number, the AIN FS provides the routing information to the CA and the call is attempted.

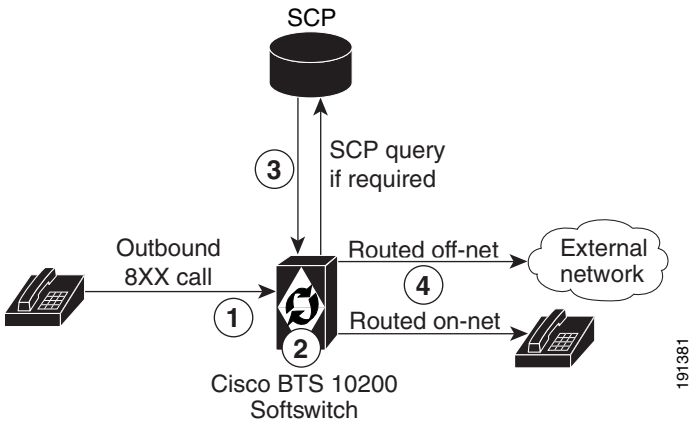
Note For an incoming 8XX call that has a network-specific NOA (based on GR-317), when the system finds the record in the internal database, it assigns the value 2 (TOLL_FREE_LOCAL) to the Database Query Type1 field in the resulting call detail record (CDR).

4. If no internal record is found, the next action depends on how the NOA token is provisioned in the dial plan table. If NOA is provisioned as NATIONAL (the default value), the AIN FS performs an external service control point (SCP) query. If a route is found, the CA completes the call. Otherwise the call is released.

Note For an incoming 8XX call that has a network-specific NOA, the system does not attempt an external query. The call is released with release cause No Route to Destination.

Figure 1-1 shows the processing of an outbound 8XX call placed by a subscriber.

Figure 1-1 Processing of an Outbound 8XX Call

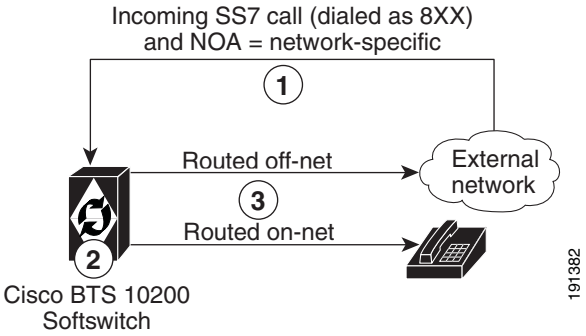


Notes for Figure 1-1

1. A subscriber dials an 8XX call.
2. The system attempts to translate the 8XX call to a DN in its local database.
3. If there is no record in the local database, the system sends a query to the SCP and receives a translated DN.
4. The system routes the call to the appropriate subscriber (on-net call) or external network (off-net call).

Figure 1-2 shows the processing of an 8XX call received from the network with a network-specific NOA.

Figure 1-2 Processing of an 8XX Call with a Network-Specific NOA



Notes for Figure 1-2

1. The system receives an incoming SS7 call with a toll-free (8XX) dialed DN and with NOA=network-specific.
2. The system attempts to translate the 8XX call to a DN in its local database.
3. The system routes the call to the appropriate subscriber (on-net call) or external network (off-net call).

Local Toll-Free Database

This section explains how the system uses information from the local toll-free database.

The BTS 10200 provides the ability to translate inbound/outbound 8XX numbers at the Feature Server (FS) using a local 8XX database. The 8XX service supports the following features:

- Origin-dependent routing
- Time-of-day routing
- Percentage-based routing
- Information digit-based screening
- Black/white list screening

The BTS 10200 also supports optional DNIS service. In an 8XX DNIS service, when a call is terminated to a PBX (call center), 4 digits are outpulsed to the PBX to identify the originally dialed 8XX number. In case of custom DNIS, up to 22 digits can be outpulsed with additional information such as:

- Original 8XX number dialed
- Automatic number identification (ANI)
- Originating line information of the calling party

When a translated number (for an original 8XX call) is received, the Analyzed Info DP triggers the FS. The BTS 10200 looks up the DNIS and TG information for the call. The DNIS information is then outpulsed to the PBX. If an overflow condition is encountered, the call is routed to the overflow trunk. The overflow trunk can be a PSTN trunk.

See SR-2275, *Telcordia Notes on the Network*, Section 14.6 for additional information on toll-free database services.

SCP-Based Toll-Free Services

This section explains how the system uses information from the external toll-free database.

The BTS 10200 communicates with an SCP-based database called the toll-free database service, which contains information for routing the call. The database service provides information about the network service provider selected to complete the call, and information for translating the toll-free number to a specific 10-digit directory number (DN). The routing of the call can vary depending on the arrangements made between the toll-free subscriber and the network service provider. These arrangements can include selective routing based on the time of day, day of week, and location from which the call originates.

Provisioning Commands

To provision this feature, see the 8XX (Toll-Free Calling) provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Active Call Information Display

The BTS 10200 allows the service provider to display information about an active (in-progress) call (originating or terminating). The implementation is based on Telcordia document *GR-529-CORE, Call Tracing (FSD 15-03-000)*. The display is performed using a CLI query command.

The input parameter can be any subscriber-specific or trunk-specific information including:

- Subscriber-specific information:
  - DN
  - TSAP address of the residential gateway (RGW)
  - MLHG ID and terminal
  - Centrex group ID and extension
  - Termination ID
- Trunk-specific information:
  - SIP call ID
  - H.323 call ID
  - Trunk group ID and trunk ID (for SS7, ISDN or CAS)

The system output (display) includes available information about the calling and called parties (for example, calling number, called number, call state, trunk type, call ID, charge number, and redirected number). The system supports both brief and verbose display modes.

For additional information about required inputs and available outputs, see the "Viewing Active Calls" information in the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

Alerting Notification to Third-Party Feature Server

The BTS 10200 can be provisioned to deliver alerting notification (notification of power ringing or call-waiting tone on the subscriber line) and call data to a third-party feature server (3PTYFS). This feature is available for both off-net-to-on-net calls and on-net-to-on-net calls. It can be assigned globally (for all subscribers on the switch), on a per-POP basis, or for individual subscribers. The feature supports advertising of an externally addressable FQDN to an external third-party feature server when necessary. The service provider can use appropriately designed and configured feature servers to make use of this notification and data to provide value-added services to subscribers; for example, delivery of caller ID on a subscriber television or computer screen.

Note Throughout this document, this feature (alerting notification to 3PTYFS) is referred to as Alerting Notification.

This document does *not* describe the messaging interface specs or call-data fields provided by the BTS 10200. Developers of applications for the 3PTYFS who are interested in the interface specifications should contact their Cisco account team.

Call Flow

The call flow works as follows:

1. The BTS 10200 receives signaling for an incoming call, and sets up the call to the subscriber line.
2. At the CALL_ACCEPTED trigger detection point (TDP) in the call, the BTS 10200 generates a CALL_ACCEPTED_NOTIFY trigger, and sends a SIP Invite message directed to a 3PTYFS. The SIP Invite message includes a Feature Control Protocol (FCP) attachment containing the call data.
3. The 3PTYFS receives the SIP message and executes any actions that have been programmed into it.

Alerting Notification has no impact on the setup or progress of the call. The BTS 10200 continues with normal call processing regardless of any response from the 3PTYFS.

Prerequisites

The BTS 10200 locates the 3PTYFS via a TSAP address that is provisioned in the BTS 10200 database. If the TSAP address is a domain name, the domain name must also be configured in the service provider domain name system (DNS) server.

The BTS 10200 advertises its own TSAP address to the 3PTYFS. There are specific requirements for entering this information during initial software installation. For details, see the "Installation Considerations" section on page 1-18.

The 3PTYFS should be provisioned to support this feature in accordance with the applicable product documentation. The BTS 10200 does not send any provisioning or status/control commands to the 3PTYFS.

Caution The data in the FCP attachment generated by the BTS 10200 is plain ASCII text and is not encrypted. The security of the connection between the BTS 10200 and the 3PTYFS is the responsibility of the service provider. It is the responsibility of the 3PTYFS to honor the presentation privacy restrictions, and control any usage or display of this information based on those restrictions.

Restrictions and Limitations

CALL_ACCEPTED_NOTIFY Trigger Sent for Incoming Calls to Subscribers Only

The system sends the CALL_ACCEPTED_NOTIFY trigger to the 3PTYFS only if the called party is a subscriber on the BTS 10200. This is true even if the feature is provisioned globally (at the office level) on the BTS 10200.

Limitations when Calling Party Is Using Certain SIP and H.323 Devices

Some calling-party devices (certain SIP- and H.323-based endpoints) may not send an explicit alerting indication (180 Ringing for SIP and Alerting for H.323). In these cases, the Call Agent does not report the CALL_ACCEPTED_NOTIFY trigger to the 3PTYFS.

Subsequent Triggers

The BTS 10200 does not send updated information to the 3PTYFS based on subsequent triggers in the call (following the CALL_ACCEPTED TDP). For example, if a user hangs up while another call is on hold (in call-waiting mode) and the phone is rung again, the BTS 10200 does not report a trigger and does not send any data.

NAPTER and SRV Record Lookup Not Supported

This feature does not support the use of the Naming Authority Pointer (NAPTR) or DNS services (SRV) records for lookup of the 3PTYFS domain name. The DNS server must be populated with the address (A) record for the fully qualified domain name (FQDN) specified in the TSAP address of the 3PTYFS.

Status and Control Commands

The **status feature-server** command reports the status of feature server components internal to the BTS 10200. However, the BTS 10200 does not send any status or control commands to the 3PTYFS.

Installation Considerations

For Alerting Notification to function correctly, specific data must be entered into the opticall.cfg file at the time of initial BTS 10200 software installation. The choice of data depends on whether the 3PTYFS will be deployed in the same private (internal) management network as the BTS 10200, or in a public network.

- If the 3PTYFS is deployed in the same private (internal) management network as the BTS 10200, the 3PTYFS can obtain the IP address of the BTS 10200 from the DNS server. That DNS entry will resolve correctly to the private IP address.
- If the 3PTYFS is deployed in a public network (outside the private management network of the BTS 10200), the 3PTYFS must reach the BTS 10200 by using an external IP address. In this case, you must populate opticall.cfg and the DNS server with the external IP address for the BTS 10200.

This installation data also affects the provisioning requirements for the 3PTYFS in the Feature Server table:

- If the 3PTYFS is deployed in the private management network, the EXTERNAL-FEATURE-SERVER parameter must be set to N.
- If the 3PTYFS is deployed in a public network, the EXTERNAL-FEATURE-SERVER parameter must be set to Y.

Note Installation of the 3PTYFS and peripheral devices is outside the scope of this document. Those devices and software should be installed according to the applicable product documentation.

Feature Provisioning Commands

For provisioning steps, see the Alerting Notification provisioning procedure in the *Cisco_BTS 10200 Softswitch Provisioning Guide*.

Calling Party Number Options for Outbound SETUP Messages

The BTS 10200 provides options for controlling the calling party number (CPN) data sent in the outbound SETUP message on calls outbound or redirected from the BTS 10200 to the PSTN.

Option to Send Billing DN as CPN for Outbound Calls

The system has a provisionable option for sending a subscriber billing DN (or main DN of a PBX subscriber) as the CPN in outbound SETUP messages on outgoing nonemergency calls. This is provisionable using the SEND-BDN-AS-CPN token in the Subscriber table.

- If SEND-BDN-AS-CPN is set to Y, the system sends the billing DN of the subscriber as the CPN in the outbound SETUP message. If the billing DN is not provisioned, the system sends the value of the subscriber directory number (DN1).
- If SEND-BDN-AS-CPN is set to N, the system sends the subscriber DN1 as the CPN in the outbound SETUP message. For PBX, the system sends the individual subscriber DN (received in the SETUP message) as the CPN in the outbound SETUP message.

The sending of the subscriber name and number is subject to the provisioning of the PRIVACY token in the Subscriber table.

Option to Send Billing DN as CPN for Emergency Calls

The system has a provisionable option for sending a subscriber billing DN (or main DN of a PBX subscriber) as the CPN in outbound SETUP messages on outgoing emergency calls. This is provisionable using the SEND-BDN-FOR-EMG token in the Subscriber table.

Note In this document, emergency calls are calls to DNs that are provisioned as call-type=EMG in the Destination table.

- If SEND-BDN-FOR-EMG is set to Y, the system sends the billing DN of the subscriber as the CPN in the outbound SETUP message. If the billing DN is not provisioned, the system sends the value of the subscriber directory number (DN1).
- If SEND-BDN-FOR-EMG is set to N, the system sends the subscriber DN1 as the CPN in the outbound SETUP message. For PBX, the system sends the individual subscriber DN (received in the SETUP message) as the CPN in the outbound setup message.

The system sends the main subscriber number, if it is provisioned, according to the following rules:

- If an ISDN PBX has main-sub-id provisioned with send-bdn-for-emg=N, send-bdn-as-cpn=N, and it is an EMG call, then the DN1 of the main-sub-id is sent as the calling party number.
- If an ISDN PBX has main-sub-id provisioned with send-bdn-for-emg=Y, send-bdn-as-cpn=N, and it is an EMG call, then the billing-dn of the main-sub-id is sent as the calling party number.

Option to Send Redirecting Number as CPN for Redirected Calls

This feature allows the service provider to control the CPN data sent in the outbound SETUP message on redirected calls outbound from the BTS 10200 to the PSTN.

The CPN option is provisionable (via CLI commands) using the SEND-RDN-AS-CPN token in the TRUNK-GRP table:

- If this token is set to Y (yes), the system overwrites the existing CPN with the redirecting number (RDN) and includes the new value in the outbound SETUP message.
- If this token is set to N (no), the system does not change the existing CPN data. N is the default value.

This feature is applicable to the following scenarios:

- Redirection by a Subscriber Phone, page 1-21
- Redirection of a Basic or Tandem Call, page 1-22

Redirection by a Subscriber Phone

Figure 1-3 shows an example of the networks and phones involved in redirection by a subscriber phone. Table 1-4 explains how to provision the SEND-RDN-AS-CPN token for various call-redirection scenarios and results.

Figure 1-3 General Network View for Redirection by a Subscriber Phone

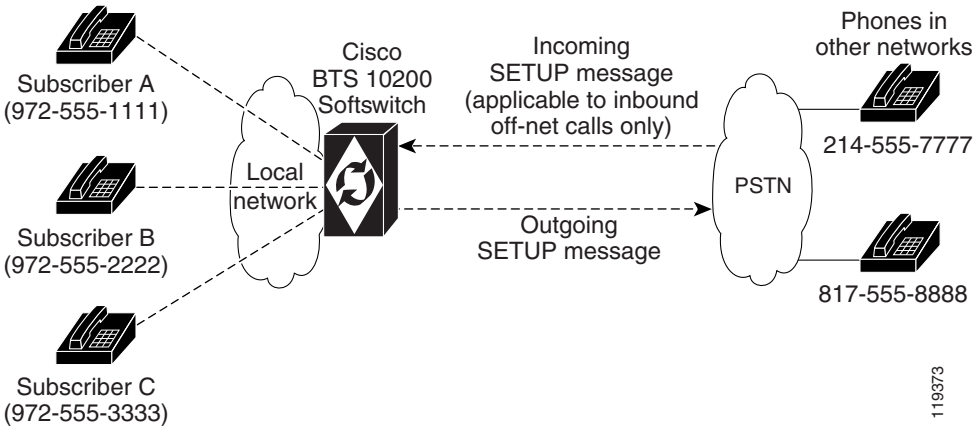


Table 1-4 Provisioning SEND-RDN-AS-CPN in TRUNK-GRP Table for Redirection by Subscriber Phone

Scenario (See Figure 1-3)	Existing CPN and RDN Data (Example)	Value Provisioned for SEND-RDN-AS-CPN	Effect On Outbound SETUP Message	Content of Outbound SETUP Data (Example)
On-net to off-net call (either of the following): A -> B -> fwd -> C -> fwd -> off-net A -> C -> fwd -> off-net	CPN= 972-555-1111 RDN= 972-555-3333	Y	Overwrite CPN with RDN	CPN= 972-555-3333 RDN= 972-555-3333
		N	Do not change CPN	CPN= 972-555-1111 RDN= 972-555-3333

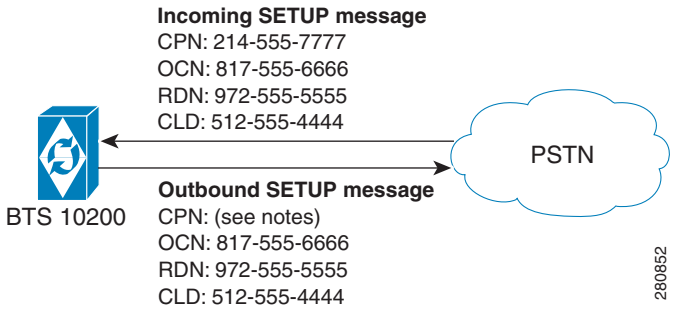
Table 1-4 Provisioning SEND-RDN-AS-CPN in TRUNK-GRP Table for Redirection by Subscriber Phone (continued)

Scenario (See Figure 1-3)	Existing CPN and RDN Data (Example)	Value Provisioned for SEND-RDN-AS-CPN	Effect On Outbound SETUP Message	Content of Outbound SETUP Data (Example)
Off-net to on-net to off-net call: Inbound off-net call -> B -> fwd -> off-net **Note** In this example, the existing RDN (from the incoming SETUP message) is 817-555-8888. The new RDN is the DN of the forwarding phone, Subscriber B—972-555-2222.	CPN= 214-555-7777 RDN= 817-555-8888 (from incoming SETUP message)	Y	Overwrite CPN with RDN	CPN= 972-555-2222 RDN= 972-555-2222
		N	Do not change CPN	CPN= 214-555-7777 RDN= 972-555-2222

Redirection of a Basic or Tandem Call

Figure 1-4 illustrates the redirection of a basic or Tandem call.

Figure 1-4 Example of Redirection of Basic or Tandem Call



Notes for Figure 1-4

- CPN = calling party number
- OCN = original called number
- RDN = redirecting number
- CLD = called number
- In this scenario, The SETUP message for the incoming call has a CLD (called number) 512-555-4444. If this number does not correspond to a subscriber, the BTS 10200 routes the call back to the PSTN according to provisioning in the dial plan. By default, the data in the outbound SETUP message (the message sent from the BTS 10200 to the PSTN) is the same as the data in the incoming SETUP message. However, if the SEND-RDN-AS-CPN parameter in the TRUNK-GRP table is set to Y, and the RDN is available in the incoming SETUP message, the system replaces the CPN value with the RDN value. Table 1-5 explains how to provision the SEND-RDN-AS-CPN token for call redirection.

Table 1-5 Provisioning SEND-RDN-AS-CPN in TRUNK-GRP Table for Redirection of Basic/Tandem Call

Scenario (See Figure 1-4)	Content of Incoming SETUP Data (Example)	Value Provisioned for SEND-RDN-AS-CPN (Default = N)	Effect On Outbound SETUP Message	Content of Outbound SETUP Data (Example)
Basic or Tandem call with RDN available in the incoming SETUP message	CPN= 214-555-7777 RDN= 972-555-5555	Y	Overwrite CPN with RDN	CPN= 972-555-5555 RDN= 972-555-5555
		N	Do not change CPN	CPN= 214-555-7777 RDN= 972-555-5555
Basic or Tandem call with RDN *not available* in the incoming SETUP message	CPN= 214-555-7777 *RDN not available*	Y	Do not change CPN	CPN= 214-555-7777 RDN not available
		N	Do not change CPN	CPN= 214-555-7777 RDN not available

Dialing Parity (IntraLATA Toll Presubscription)

The BTS 10200 supports this feature in accordance with Telcordia document GR-693-CORE, LSSGR: *Presubscription Indication (FSD 20-24-0000)*.

Dialing parity—also known as intraLATA toll presubscription—allows subscribers to select a telecommunications company for intraLATA calls (local toll calls) in the same way they select a long-distance provider. With dialing parity, subscribers are able to dial the number they want and have a preselected carrier—a competitive local exchange carrier (CLEC), incumbent local exchange carrier (ILEC), or a long-distance carrier—automatically handle the call if it is a local (intraLATA) toll call. Preselecting a local toll carrier eliminates the need for dial-around service for local toll calls (101XXXX numbers). Prior to implementation of dialing parity, long-distance carriers provided intraLATA service by dialing around an ILEC or CLEC via 101XXXX numbers (carrier access codes—CACs).

Local access and transport areas (LATAs) were created after the breakup of the AT&T system. LATAs are also known as called service areas or local toll calling areas. CLECs and ILECs provide two types of calls to their subscribers within the LATA:

- Local calls
- Local toll calls

Local toll calls are typically calls to places more than 16 miles from the subscriber location in urban areas and more than 13 miles in rural areas. Local toll calls do not qualify as either local or long distance—they are between the two and are subject to different rates.

Local Number Portability (LNP)

The BTS 10200 supports local number portability (LNP) for North American and ITU-based systems. For general information, see *Number Portability Switching Systems*, T1.TRQ-02-2001, which provides unofficial agreement within T1S1. T1S1 is the ATIS accredited body for signaling. This document is available at http://www.atis.org.

LNP permits subscribers who change their local phone company to keep their existing telephone numbers. An FCC order requires this feature in the 100 top metropolitan service areas in the United States. LNP permits calls to be routed to the subscriber's new local switch without any particular per-call action required of either the calling or called party. Each switch contains a database of the office codes (NPA-NXXs) associated with subscriber numbers that have been ported in and ported out.

Note The LNP feature can be made available to all subscribers lines connected to a BTS 10200 using the default office service ID, or to all subscribers in a specific POP using the office service ID. See the "Office Service ID and Default Office Service ID" section on page 3-134 for a general description of this provisionable service.

The BTS 10200 supports the LNP function as follows:

- Ranges/blocks of ported numbers are provisionable in the BTS 10200, with block size granularity from 100 to 10,000 DNs per block.
- During the call processing, if the dialed digits/destined digits match 3 to 10 contiguous digits of a ported NPA-NXX-XXXX at the Info_Analyzed/ Collected_Info trigger detection point (TDP), a query is initiated to an external database using the AIN Info_Analyzed message. This LNP trigger is also known as the public office dialing plan (PODP) trigger.
- The BTS 10200 processes the received response (Analyze_Route) from the TCAP query and determines whether the dialed digits have been translated to a location routing number (LRN):
  - If the CalledPartyID received from the Analyze_Route differs from the dialed digits (that is, the LRN comes back), the call is routed based on the received CalledPartyID as the ISUP IAM CalledPartyNumber and sets the ForwardCallIndicator parameter to "Number translated". The ISUP IAM also includes the ISUP Generic Address Parameter (GAP) set to the dialed digits.
  - If the CalledPartyID received from the Analyze_Route is the same as the dialed digits (that is, no LRN comes back), the call is routed based on the received CalledPartyID as the ISUP IAM CalledPartyNumber and sets the ISUP ForwardCallIndicator (FCI) parameter to "Number translated".
  - When the LNP query results in an error, the call is routed based on the dialed digits/destination digits, and does not include the ISUP GAP, and the FCI is set to "Number not translated".

For a comprehensive description of LNP functions and provisionable parameters, see the *Cisco BTS 10200 Softswitch Dial Plan Guide*.

To provision LNP options, see the appropriate procedures in the *Cisco BTS 10200 Softswitch Provisioning Guide*:

- Local Number Portability (LNP) for ANSI/North America
- Local Number Portability (LNP) ITU Local BTS Database Query
- SS7 Provisioning

RFC 2833 DTMF Relay—Call Agent Controlled Mode

The system supports Call Agent (CA) controlled mode for dual tone multifrequency (DTMF) relay based on RFC 2833. During call setup, the CA (the BTS 10200) can authorize an embedded multimedia terminal adapter (eMTA) or media gateway (MGW) to invoke RFC 2833 DTMF relay procedures.

Note Prior to Release 5.0, RFC 2833 DTMF relay was not controlled by the Call Agent (the BTS 10200), therefore invocation of RFC 2833 DTMF relay was based on the configuration in the individual eMTA or MGW.

This feature affects MGCP, NCS, TGCP, SIP, and H.323 gateways and endpoints connected to the BTS 10200. The implementation is compliant with the following requirements from industry standards:

- Section 7.1.1 of PKT-SP-NCS1.5-I01-050128
- Section 7.1.1 of PKT-SP-TGCP1.5-I01-050128

Interfaces

The following interfaces are supported for this feature:

- NCS-based eMTA subscribers
- MGCP-based and TGCP-based TGWs (SS7, ISDN, CAS)
- MGCP-based subscribers

Protocol Interworking

This feature can be invoked on the following types of calls:

- MGCP(subscribers and trunks) <-> NCS(subscribers)
- MGCP(subscribers and trunks) <-> H.323(endpoints and trunks)
- NCS(subscribers) <-> H.323(endpoints and trunks)
- MGCP(subscribers and trunks) <-> SIP(subscribers and trunks)
- NCS(subscribers) <-> SIP(subscribers and trunks)
- SIP(subscribers and trunks) <-> H.323(endpoints and trunks)
- MGCP(subscribers and trunks) <-> MGCP(subscribers and trunks)
- H.323(endpoints and trunks) <-> H.323(endpoints and trunks)
- SIP(subscribers and trunks) <-> SIP(subscribers and trunks)
- NCS(subscribers) <-> NCS(subscribers)

The BTS 10200 sends the RFC 2833 DTMF relay parameters to the MGW or endpoint when setting up the initial call and also when setting up features involved in the call, for example forwarded calls.

In addition to configuring the BTS 10200, you must also configure the gateways and endpoints appropriately for the desired features.

Availability of Legacy Behavior

An endpoint can send RFC 2833 DTMF parameters in the Session Description Protocol (SDP) message based on the configuration in the endpoint and without control of the CA. This legacy behavior can be preserved by accepting the default values of the following parameters in the BTS 10200 database:

- In the qos table, dtmf-telephone-event-enabled defaults to N.
- In the h323-tg-profile and h323-term-profile tables, rfc2833-payload defaults to 98.

- In the mgw-profile table, dtmf-telephone-event-supp defaults to AUTO.

Limitations

This section discusses limitations on the implementation of this feature.

Limitations Based on Interactions with Out-Of-Band Digit Transmission

The BTS 10200 assigns a higher priority to the authorization of RFC 2833 DTMF relay than to the authorization of out of band (OOB) digits. If both RFC 2833 and OOB support are enabled in the qos and mgw-profile tables, the system sends RFC 2833 authorization but not OOB authorization. However, the actual implementation of RFC 2833 or OOB implementation depends on the configuration of the two endpoints in the call. If an endpoint specifically requests the use of OOB digits (for example, a SIP subscribe/notify case), the BTS 10200 requests OOB digits also.

Limitations on CA Control

The implementation of RFC 2833 DTMF relay in a specific call depends on payload negotiation by the two endpoints in the call. The following two cases illustrate the limitations on the control exercised by the CA:

- If the BTS 10200 sends authorization during call setup, but the two endpoints cannot successfully negotiate payload parameters, RFC 2833 DTMF relay is not performed.

  For MGCP, NCS, and SIP endpoints, payload negotiation is done through SDP exchange. For H.323 endpoints it is done through H.245 messages.

- If the BTS 10200 *does not send* RFC 2833 DTMF relay authorization during call setup, but one of the endpoints sends SDP messages containing RFC 2833 attributes, the BTS 10200 passes the attributes through to the other endpoint. In such a case. the two endpoints might negotiate payload parameters, and RFC 2833 DTMF relay could be performed.

Limitations on Interoperability with Other NEs

The BTS 10200 interworks with a wide range of network elements (NEs), but there are certain limitations. We recommend that you keep the following caution in mind as you prepare to purchase and use NEs for your network.

Caution Some features involve the use of other network elements (NEs) deployed in the service provider network, for example, gateways, media servers, SIP devices, and eMTAs. See the "Component Interoperability" section of the *Cisco BTS 10200 Softswitch Release Notes* for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the BTS 10200 Release 5.0 software. Earlier or later releases of platform software might be interoperable and it might be possible to use other functions on these platforms. The list in the *Release Notes* certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the BTS 10200.

Conditions for Sending LCO for RFC 2833 Telephone-Events

The following conditions apply to BTS 10200 messaging for RFC 2833 telephone-events to the originating and terminating sides in the call. The implementation of these capabilities depends upon the provisioning of certain parameters in the database.

- If the originating side does not support RFC 2833, the BTS 10200 does not send telephone-events to the terminating side even if the terminating side supports RFC 2833.
- If the originating side supports RFC 2833, the BTS 10200 sends telephone-events to the terminating side before checking whether the terminating side supports RFC 2833.
- If the originating side supports RFC 2833, but the DTMF flag in the mgw-profile table is set to N, the BTS 10200 does not send telephone-events to either side.

If the originating endpoint is NCS, MGCP, or TGCP based, the BTS 10200 sends a create-connection (CRCX) message containing the local connection option (LCO) for RFC 2833 telephone-events if the originating endpoint is provisioned in the BTS 10200 with:

- qos table—dtmf-telephone-event-enabled=y
- mgw-profile table—One of the following is true: (1) dtmf-telephone-event-supp=y, *or* (2) dtmf-telephone-event-supp=auto and the endpoint reports the telephone-event codec in the AUEP ACK message.

The system can also send a CRCX message containing the LCO for RFC 2833 telephone-events if the terminating and originating endpoints are both MGCP based, or if both endpoints are NCS or TGCP based, and the following parameters are provisioned in the BTS 10200:

- Both endpoints are provisioned with codec-neg-supp=y in the mgw-profile table.
- The terminating endpoint is provisioned with:
  - qos table—dtmf-telephone-event-enabled=y
  - mgw-profile table—One of the following is true: (1) dtmf-telephone-event-supp=y, *or* (2) dtmf-telephone-event-supp=auto and the endpoint reports the telephone-event codec in the AUEP ACK message.

SIP Triggers

This section explains the scope of the SIP Triggers feature and provides a technical description of it.

Scope for Release 5.0

Release 5.0 of the BTS 10200 supports the following SIP triggers:

- Off-hook trigger with provisionable delay (OHD):
  - Supported for MGCP and NCS subscribers
  - *Not* supported for SIP endpoints (SIP subscribers)
- Termination Attempted Trigger 1 (TAT_1) and Termination Attempted Trigger 2 (TAT_2):
  - Supported for MGCP and NCS subscribers.
  - Release 5.0, MR1 and later. Supported for SIP endpoints (SIP subscribers) when the incoming call is based on a DN.

Feature Limitations

SIP triggers are not supported for Centrex subscribers.

The system does not support the OHD trigger for SIP subscribers.

The BTS 10200 does not invoke any SIP triggers for SIP subscribers on incoming calls that are based on an address of record (AOR).

Technical Description of SIP Triggers

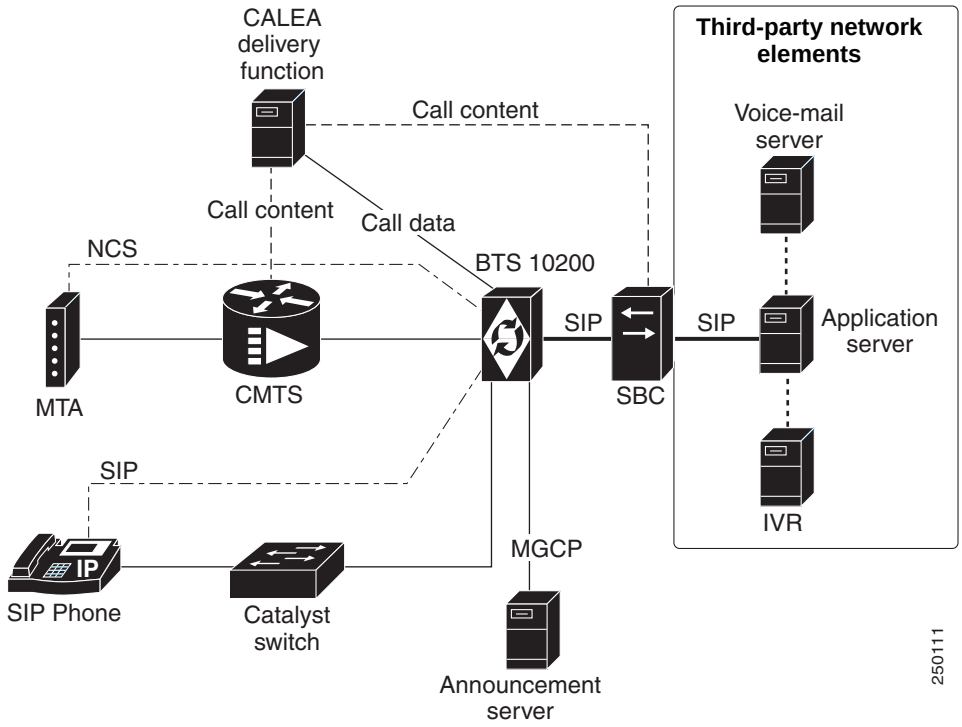
The SIP Triggers feature uses the SIP protocol, with some extensions, to enable the BTS 10200 to interoperate with third-party application servers so that Multi-Service Operators (MSOs) can provide customers with enhanced features and services. The triggers can be used by the third-party servers to provide originating services (such as voice dial) when a subscriber places a call, and enhanced terminating services (such as TV caller ID and custom ringback) when a subscriber receives a call.

The BTS 10200 supports multiple application servers. Application servers are provisioned per subscriber origination and subscriber termination. This section describes the triggers that enable this interoperation with the third-party application servers.

You can provision SIP triggers on an individual subscriber level on the BTS 10200.

Figure 1-5 shows a typical network architecture for SIP triggers, including the connection between the BTS 10200 and the third-party application server. The capability to provide TAT_1 and TAT_2 SIP triggers to SIP phones is available in Release 5.0 MR1 and later.

Figure 1-5 Typical Network Architecture for SIP Triggers



Acronyms for Figure 1-5

CALEA—Communications Assistance for Law Enforcement Act

NCS—Network-based call signaling

SBC—Session border controller

CMTS—Cable modem termination system

IVR—Interactive voice response

Terminology Used in This Section

The following terminology is used in this section:

- TAT_1 and TAT_2—Termination attempt triggers, collectively referred to as TAT in this document. These triggers occur at different points in the call; TAT_1 occurs before TAT_2, and can be used by an external application server to provide specific services at specific points in the call. These triggers are provisioned as fname=TAT_1 and fname=TAT_2.
- OHD—Off-hook trigger with provisionable delay. The OHD trigger for each subscriber can be designated as off-hook immediate (OHI) or off-hook delayed (OHD). You provision this through the offhook-trigger-type parameter in the Subscriber table:
  - OHD occurs when a provisionable timer runs out after the caller goes off-hook.
  - OHI occurs immediately after the caller goes off-hook.

Tip There is an OHD trigger provisioned as fname=OHD in the Feature table, and there is a delayed or immediate designation provisioned as offhook-trigger-type=OHD or OHI in the Subscriber table.

Off-Hook Trigger (Delayed and Immediate)

The OHD trigger occurs either immediately after the user goes off-hook (if offhook-trigger-type=OHI) or after a delay set through a configurable timer (if offhook-trigger-type=OHD).

- If off-hook immediate is provisioned, the BTS_10200 establishes a connection to the external application server provisioned for that combination of subscriber and trigger and sends the call to the server immediately after the caller goes off-hook.
- If off-hook delayed is provisioned and the user goes off-hook, dial tone is provided to the subscriber for the configured number of seconds. When the delay timer expires, dial tone is stopped, and the BTS 10200 establishes a connection to the external application server provisioned for that combination of subscriber and trigger and sends the call to the server. If the user starts dialing before the delay timer expires, the BTS 10200 allows digit collection to be completed before establishing the connection to the application server. Depending on the service invoked (for example, dial by name), the application server determines the desired called party and sends the call back to the BTS 10200 to continue originating processing.

The BTS 10200 inserts two route headers in the INVITE that is sent to the application server:

- Topmost route header—Intended for the application server so that it can identify the logic to be executed on the application server. This header can be provisioned on the BTS 10200 per subscriber or set with a default for all OHD subscribers.
- Return route header—Identifies the necessary call session and processing information when the INVITE is returned to the BTS 10200. This route header must be returned unchanged to the BTS 10200 in the INVITE that is sent from the application server to the BTS 10200.

Termination Attempt Triggers (TAT_1 and TAT_2)

The TAT trigger occurs when a call terminates to a BTS 10200 subscriber who has one or both TAT triggers (TAT_1 and TAT_2) enabled. The BTS 10200 sends the terminating call to the external application server before ringing the subscriber. The application server may provide services such as screening or custom ringback. If the application server determines that the call should be offered to the subscriber, it sends the call back to the BTS 10200 to continue termination processing.

The TAT triggers operate as follows:

- The TAT_1 trigger takes precedence over all other BTS 10200 terminating features at the TERMINATION_ATTEMPT_AUTHORIZED trigger detection point. However, if the CNAM TCAP query is provisioned for a subscriber, it is performed before the TAT_1 trigger, and the name is provided to the application server. The BTS 10200 honors the calling name it receives from the application server and does not launch a CNAM query if the name is presented by the application server.
- The TAT_2 trigger is the last feature invoked at the TERMINATION_ATTEMPT_AUTHORIZED trigger detection point.

A TAT trigger is not disabled even if the user is in an Emergency call. However, a return INVITE from the application server fails at the BTS 10200 if the user is in an Emergency call.

As it processes a TAT, the BTS 10200 manages the following events:

- Successful application server invocation
- Unsuccessful application server invocation
- Application server terminates call
- Application server sends call back to the BTS 10200 for termination processing

The system populates two Route headers in the INVITE it sends to the application server. The contents of the Route headers are controlled by provisioning. The provisioning of the first Route header is determined by the requirements of the application server and that of the second is determined by the requirements of the BTS 10200. The following examples illustrate the format of the Route field, with both the first Route header and return Route header shown in the example:

Examples—Route Message:

```
Route: <topmost route>,<return route>;service-ref=SCM0579081256

Route: <sip:TAT_1-app@APP_SERVER1.serviceprovider.com;lr>,
<sip:TAT_1@bts1.serviceprovider.com;lr>;service-ref=SCM0579081256

Route: <sip:TAT_2-app@APP_SERVER1.serviceprovider.com;lr>,
<sip:TAT_2@bts1.serviceprovider.com;lr>;service-ref=SCM0537491333
```

Note The meaning of lr in the route message is loose routing. See RFC 3261 for a description.

Subscriber Features

The following are examples of services that could be offered in conjunction with the TAT and OHD triggers if there ia an appropriate application server in the network:

- Voice menu (OHD trigger)
- Voice dialing (OHD trigger)

- Multi-party voice dialing (OHD trigger)
- TV caller ID, with or without picture (TAT trigger)
- Custom ring-back tone (TAT trigger)
- Enhanced voicemail UI (OHD trigger)
- Message status (OHD trigger)
- Missed call status (OHD trigger)
- Voicemail screening (specific digit string (vertical service code))
- Smart call forward (TAT trigger)
- Smart call return (OHD trigger)
- Dialpad sound effects (specific digit string)
- Multi-ring call forward (TAT trigger)
- Click to dial (third-party call control [3PCC] mechanisms)

Note Support of subscriber services is not limited to those identified in the preceding list.

Failover Behavior

During transitions (for example, while the call to the application server is being placed or while the call from the application server is placed to the destination), a failover of the call agent or feature server is likely to cause the call to be dropped.

If a call is connected to the application server, or if a call is connected end to end, a failover of the call agent or feature server does not disrupt the call.

Feature Interactions for OHD Trigger

The OHD trigger is supported for MGCP and NCS subscribers, but not for SIP subscribers.

Features that are provided by the application server interwork with the features provided by the BTS 10200. Table 1-6 describes the feature interactions for the OHD trigger.

Table 1-6 Feature Interactions for OHD Trigger

Feature	Abbreviation	Interaction
Vertical Service Codes (VSCs): • Activation, deactivation, and interrogation features, including the use of VSCs, for example AC_ACT, AC_DEACT, CBLK, CCW, COT, CFUA, CFBI, CNAB, CNDB, DND_ACT, and DND_DEACT. • VSCs dialed to access feature management functions, for example PS_MANAGE, PS_O, CIDSD, CIDSS, VM_ACCESS. • Initial VSCs entered by the handset user to invoke AC and AR.	(various)	If the user dials the VSC during the dial tone, the BTS 10200 collects the VSC digits and then forwards the call to the application server. If the user dials the VSC after the BTS 10200 establishes the call to the application server, the application server collects the VSC digits. The application server is configured to send the REFER back to the BTS 10200 with the VSC if it is not capable of handling this VSC. When the REFER is received by the BTS 10200, the BTS 10200 provides origination processing. During origination processing, if more digits must be collected, the BTS 10200 does so by playing appropriate tones directly at the endpoint. After the process (activation, deactivation, interrogation, or feature management) is complete, the BTS 10200 does not invoke SIP triggers to the application server again.
Toll Free	8xx	OHD trigger takes precedence.
Emergency Service	911	Emergency calls are routed to the application server if the BTS 10200 Call Agent Configuration table is provisioned to do so: `add ca-config type=EMG-ROUTE-TO-AS; datatype=BOOLEAN; VALUE=Y;` If EMG-ROUTE-TO-AS is set to N (default), the BTS 10200 processes the call locally and does not invoke the application server. If EMG-ROUTE-TO-AS is set to Y and the dialed digits match the digit string provisioned in the **emergency-number-list** table, the BTS 10200 can route the call to the application server. The actual treatment of the call is as follows: • If the user dials the emergency number before the call is connected to the application server, the BTS 10200 processes the call locally and does not invoke the application server. • If the user dials the emergency number after the call is connected to the application server, the application server is expected to collect the digits and send a REFER or return INVITE to the BTS 10200. When the BTS 10200 receives the REFER or return INVITE, it makes the call to the emergency number.
Automatic Callback	AC	When the subscriber enters the VSC on the handset, the BTS 10200 invokes the OHD trigger. When the BTS 10200 calls back the subscriber, the callback does not invoke OHD. When the BTS 10200 sets up the final call to the remote phone, it treats this as a new call and invokes the OHD trigger to the application server.
Automatic Recall	AR	Same as AC.

Table 1-6 Feature Interactions for OHD Trigger (continued)

Feature	Abbreviation	Interaction
Class of Service	COS	OHD takes precedence, and COS screening is applied after the return INVITE is received at the BTS 10200. Authorization Code and Account Code features are already being supported by use of IVR. Therefore, these features, if needed, can be configured on the BTS 10200 to be supported by IVR.
Call Transfer	CT	A second origination attempt also goes through the application server.
Hotline	HOTLINE	If HOTLINE and OHD are active, the hotline number is expanded and the number is included in the request URI user part sent to the application server.
Hotline Variable	HOTV	Same as Hotline.
Limited Call Duration	LCD	OHD takes precedence and the process of checking the prepaid server occurs after the return INVITE is received from the feature server.
Local Number Portability	LNP	OHD takes precedence and a local number portability query is invoked after the return INVITE is received from the feature server.
Outgoing Call Barring	OCB	OHD takes precedence and OCB is applied after the application server sends the call back to the BTS 10200.
Speed Call - 1 /2 digit	SC1D SC2D	The call is routed to the application server with the speed-dial digits. When the return INVITE is received from the application server, the BTS 10200 provides the speed call function.
Three Way Call	TWC	The second origination attempt goes to the application server.
Three Way Call Deluxe	TWCD	Same as TWC.
Usage Sensitive Three Way Call	USTWC	Same as TWC.
Warmline	WARMLINE	If warm line and OHD are provisioned, the warmline number is included in the INVITE message (user part of request URI) to the application server. **Note** If a subscriber is provisioned for both warmline and OHD, the delay for OHD should not be used. Either the subscriber dials before the warmline timeout and the dialed number is provided to the application server, or the warmline timeout occurs, and the warmline number is provided to the application server. The application server does not collect digits. Off Hook Immediate is not available. Speak to Dial is not available. Similarly, the offhook delay timer for OHD is not used if hotline is also active. If both OHD and hotline are active, the BTS 10200 immediately sends an INVITE to the application server that includes the provisioned hotline number. The user does not receive an initial dial tone.

Feature Interactions for TAT_1 and TAT_2 Triggers

TAT_1 and TAT_2 triggers are supported for MGCP and NCS subscribers in the initial release of Release 5.0, and also supported for SIP subscribers in Release 5.0 Maintenance Release 1 (MR1) and later.

Features that are provided by the application server interwork with the features provided by the BTS 10200. Table 1-7 describes the feature interactions for the TAT_1 and TAT_2 triggers.

Caution It is the responsibility of the application server to honor the privacy settings of the calling party based on the information received in the message from the BTS 10200 for the TAT_1 and TAT_2 triggers.

Table 1-7 Feature Interactions for TAT_1 and TAT_2 Triggers

Feature	Abbreviation	Interaction for MGCP and NCS Subscribers	Interaction for SIP Subscribers (Release 5.0 MR1 and Later)
Emergency-Service	911	If the called user is already in an emergency call, and the BTS 10200 receives an additional incoming call for this user, the TAT trigger is invoked, and the BTS 10200 sends the new call information to the application server. The application server might send a return INVITE. If the user is in the emergency call when the BTS 10200 receives the return INVITE, the BTS 10200 fails the new incoming call.	Same as for MGCP/NCS
Anonymous Call Rejection	ACR	The order of precedence for the triggers is TAT_1, ACR, TAT_2. If the call is rejected by ACR, TAT_2 is not invoked.	If the feature is provided by the SIP endpoint, the TAT_1 and TAT_2 triggers are invoked normally. If the feature is provided by the BTS 10200, the interaction is the same for SIP subscribers as for MGCP/NCS subscribers.
Busy Line Verification	BLV	BLV takes precedence and the TAT trigger is not invoked.	BLV is not supported for SIP subscribers.
Call-Forwarding-Busy/ Call-Forward-No-Answer/ Call Forwarding Combined/ Call-Forwarding-Unconditional - Invocation	CFB/CFNA/ CFC/CFU Invocation	The order of precedence for the triggers is TAT_1, CFU, TAT_2, [CFB/CFNA/CFC].	Same as for MGCP/NCS **Note** The reminder ring is not provided for SIP subscribers, but this does not change the feature interaction.
Calling Identity Delivery on Call Waiting	CIDCW	The TAT takes precedence over CIDCW, and the return INVITE from application server results in CW.	For SIP subscribers, CIDCW is a SIP endpoint feature, not a feature of the BTS 10200.

Table 1-7 Feature Interactions for TAT_1 and TAT_2 Triggers (continued)

Feature	Abbreviation	Interaction for MGCP and NCS Subscribers	Interaction for SIP Subscribers (Release 5.0 MR1 and Later)
Calling Name Delivery	CNAM	The CNAM query is performed before the TAT is invoked.	Same as for MGCP/NCS
Calling Number Delivery	CND	The application server is a trusted entity; therefore, the calling number is always delivered to the application server.	Same as for MGCP/NCS
Call Waiting	CW	The TAT takes precedence over CW, and the return INVITE from application server results in CW.	For SIP subscribers, CW is a SIP endpoint feature, not a feature of the BTS 10200.
Call Waiting Deluxe	CWD	Same as CW.	Same as CW.
Do Not Disturb	DND	TAT_1 takes precedence and the BTS 10200 invokes DND after it receives the return INVITE from the application server. **Note** DND takes precedence over TAT_2.	If the feature is provided by the SIP endpoint, the TAT_1 and TAT_2 triggers are invoked normally. If the feature is provided by the BTS 10200, the interaction is the same for SIP subscribers as for MGCP/NCS subscribers.
Distinctive Ringing Call Waiting	DRCW	The order of precedence for the triggers is TAT_1, TAT_2, DRCW.	Same as for MGCP/NCS
No Solicitation Announcement	NSA	The order of precedence for the triggers is TAT_1, NSA, TAT_2.	Same as for MGCP/NCS
Privacy Screening	PS	The order of precedence for the triggers is TAT_1, PS, TAT_2.	Same as for MGCP/NCS
Remote Call Forwarding	RCF	The TAT_1 trigger takes precedence over RCF.	Same as for MGCP/NCS
Selective Call Acceptance/ Selective Call Forwarding/ Selective Call Rejection	SCA/SCF/SCR	TAT_1 takes precedence, and the BTS 10200 invokes SCA/SCF/SCR after it receives the return INVITE from the application server. **Note** SCA/SCF/SCR takes precedence over TAT_2.	Same as for MGCP/NCS
Voicemail	VM	The order of precedence for the triggers is TAT_1, VM, TAT_2.	Same as for MGCP/NCS
Voicemail Always	VMA	The TAT_1 trigger takes precedence over VMA.	Same as for MGCP/NCS

Billing

The following call detail block (CDB) billing fields report the SIP originating and terminating context IDs. Details of these CDBs are provided in Appendix A of the *Cisco BTS 10200 Softswitch Billing Guide*.

- CDB field 232, SIP Originating Context Id
- CDB field 233, SIP Terminating Context Id

The following call data fields are provided for SIP triggers. Details regarding the information in these fields are provided in Chapter 2, "Feature Server Derived Call Data," of the *Cisco BTS 10200 Softswitch Billing Guide*.

- SIP Off-Hook Trigger
- SIP Termination Attempt Trigger

Provisioning Commands

The provisioning steps for this feature are based on the provisioning steps for SIP triggers for NCS endpoints in the *Cisco BTS 10200 Softswitch Provisioning Guide*, with the following exception—SIP triggers for SIP endpoints include only the terminating attempt triggers (TAT_1 and TAT_2), not the off-hook trigger (OHD). When you provision SIP endpoints, include all of the provisioning for TAT-related parameters, and exclude any provisioning for OHD-related parameters.

Error Handling

This section describes how the BTS 10200 operates when it receives 4xx, 5xx, and 6xx responses over the IP Multimedia Subsystem (IMS) Service Control (ISC) interface from the application server.

Table 1-8 lists the response codes and indicates how the BTS 10200 operates when it receives 4xx, 5xx, and 6xx responses over the ISC/application server interface.

Table 1-8 uses the following terms:

- Continue—Indicates that the BTS 10200 processes the call locally. In the case of the OHI or OHD trigger with no digits, the BTS 10200 prompts the user, collects the address digits, and then processes the call locally.
- Error treatment—Indicates that the BTS 10200 connects the user to a configured tone or announcement and then disconnects the call.

Table 1-8 BTS 10200 Management of Error Response Codes

Response Code	OHI or OHD with No Digits	OHD with Digits, TAT
400—Bad Request	Continue	Continue
401—Unauthorized	Continue	Continue
402—Payment Required	Continue	Continue
403—Forbidden	Continue	Error treatment
404—Not Found[1]	Continue	Continue
405—Method Not Allowed	Continue	Continue
406—Not Acceptable	Continue	Continue
407—Proxy Authentication Required	Continue	Continue

Table 1-8 BTS 10200 Management of Error Response Codes (continued)

Response Code	OHI or OHD with No Digits	OHD with Digits, TAT
408—Request Timeout	Continue	Continue
410—Gone	Continue	Error treatment
413—Request Entity Too Large	Continue	Continue
414—Request URI Too Large	Continue	Continue
415—Unsupported Media Type	Continue	Continue
416—Unsupported URI Scheme	Continue	Continue
420—Bad Extension	Continue	Continue
421—Extension Required	Continue	Continue
423—Interval Too Brief	Continue	Continue
480—Temporarily Unavailable	Continue	Continue
481—Call/Transaction Does Not Exist	Continue	Continue
482—Loop Detected	Continue	Error treatment
483—Too Many Hops	Continue	Continue
484—Address Incomplete	Continue	Error treatment
485—Ambiguous	Continue	Continue
486—Busy Here	Continue	Error treatment
487—Request Terminated	Continue	Error treatment
488—Not Acceptable Here	Continue	Continue
491—Request Pending	Continue	Continue
493—Undecipherable	Continue	Continue
500—Server Internal Error	Continue	Continue
501—Not Implemented	Continue	Continue
502—Bad Gateway	Continue	Error treatment
503—Service Unavailable	Continue	Continue
504—Server Timeout	Continue	Continue
505—Version Not Supported	Continue	Continue
513—Message Too Large	Continue	Continue
600—Busy Everywhere	Continue	Error treatment
603—Decline	Continue	Error treatment
604—Does Not Exist Anywhere	Continue	Error treatment
606—Not Acceptable	Continue	Error treatment

1. The application server might send a 404 or 305 response code if the user is not subscribed to the requested service (feature). If a 305 is returned, the FQDN of the contact header received in the 305 must be of the receiving BTS 10200. Receiving the 305 prompts the BTS 10200 to continue to process the call locally without reengaging the application server. If the BTS 10200 receives a 404 response code, it continues to process the call locally. The 404 also might be generated by a downstream node; but, the BTS 10200 is not able to differentiate if the 404 is generated by the application server or the downstream node. Therefore, attempting to process the call locally might fail again. The number of times that the BTS 10200 reattempts this "failed call" can depend on the number of triggers executed before the 404 error is encountered. In the worse case, if a user is configured with OHD, TAT_1, and TAT_2, the BTS 10200 can reattempt the call four times before the caller is connected to error treatment.

Split-NPA

When DNs are exhausted within an NPA, an additional NPA is assigned to the region. The new NPA may be allocated as an overlay over the existing NPA, in which case there is no major impact to the BTS 10200. However, when the new NPA is assigned based on a geographical split of the region, there are significant impacts. The assignment of the new NPA based on a geographical split is referred to as split-NPA.

The split-NPA feature impacts both provisioning (EMS) and call processing subsystems in the BTS 10200. Several provisioning tasks must be performed to introduce a new NPA into a region, including:

- Duplicate records (tasks to be performed before permissive period)
- Update ANI records (tasks to be performed during permissive period)
- Cleanup (tasks to be performed after permissive period)

Note The permissive period is the time frame where both old NPA and the new NPA can be dialed to reach the subscribers affected due to the split-NPA feature.

Before the permissive period begins, subscribers affected due to the split-NPA can be reached only via the old NPA. Duplicate records for both old and new NPA are created before the permissive period begins.

During the permissive period, both old and new NPA can be dialed (10-digit dialing is required to reach a subscriber in the affected NPA). The subscriber (ANI) and subscriber feature data records are updated to the new NPA during the permissive period.

Once the permissive period ends, subscribers affected due to the split-NPA can be reached only via the new NPA. This is referred to as the mandatory dialing period for the new NPA. The duplicate records created before the permissive period are cleaned up after the mandatory period begins.

For additional information on split-NPA, see the ATIS document INC97-0404-016, *NPA Code Relief Planning & Notification Guidelines*.

Note The split-NPA feature does recognize a leading digit (example: 9) that has been provisioned to represent a centrex subscriber DN. The only leading digit that the split-npa feature takes into account is the leading "1" digit.

Feature Provisioning Commands

To provision this feature, see the Split NPA provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

T.38 Fax Relay, Modem, and TDD Handling

This section describes the BTS 10200 fax, modem, and Telecommunications Devices for the Deaf (TDD) handling feature.

The Cisco BTS 10200 Softswitch supports ITU-T T.38 procedures on the following interfaces:

- NCS MTA subscribers

- MGCP subscribers
- MGCP (or TGCP) trunking gateways (SS7, ISDN)
- H.323 trunks

  T.38 fax is supported for the following H.323 configurations:

  - H.323 trunk using fast connect procedure (fast start)
  - H.323 trunk using non-fast connect procedure (slow start)
  - H.323 trunk using gatekeeper (H.225 RAS messaging)
  - H.323 trunk not using gatekeeper (direct trunks)
  - H.323 trunk with and without H.245 tunneling enabled
- SIP trunks
- RFC 3261-compliant SIP endpoints

Following is a list of industry references for T.38 fax relay

- ITU-T Recommendation T.38 (06/98) - *Procedures for Real-Time Group 3 Facsimile Communication Over IP Networks*.
- ITU-T Recommendation T.38 Annex D - *SIP/SDP Call Establishment Procedures*.
- F. Andreasen, draft-andreasen-mgcp-fax-04.txt, August 2004, *FXR: MGCP Fax Package*.
- H.323 Specification - Annex D - Version 2 (also incorporated into H.323 Version 4).

This section covers the following topics:

- Understanding the Fax, Modem, and TDD Handling Feature
- MGCP/NCS Interface—Fax Modes Supported
- SDP Attributes Support for T.38 Fax Relay
- MTA DQOS Support for T.38 Fax Relay
- Fallback to Audio Media on T.38 Negotiation Failure
- Audio Restore After Successful T.38 Fax Transmission
- T.38 Glare Handling
- SDP Attributes Encoding Formats
- SIP Support for Call Legs
- Protocol Interworking
- TDD Handling
- Control Configuration
- Restrictions and Limitations
- Feature Provisioning Commands

Understanding the Fax, Modem, and TDD Handling Feature

Voice Over Internet Protocol (VoIP) converts sounds into data; when converting, tones are lost. To fix the issue of lost tones the ITU developed the T.38 standard. T.38 converts sounds into data without losing these tones. Fax, modem, and TDD communications do not need the same kind of treatment voice calls do. Upspeed carries fax, modem, and TDD calls in-band over a voice call without the overhead of a G.729 codec and voice-enhancing features.

BTS 10200 Call Agents (CAs) manage calls and control media gateways (MGWs). A gateway can be the BTS 10200 itself or another device, like a Multimedia Terminal Adapter (MTA) or an Integrated Access Device (IAD). Using different modes on the BTS 10200, you can set gateways to do the following upon receiving fax, modem, or TDD tones:

- Use (upspeed) the G.711 codec
- Turn off silence suppression, echo cancellation (EC), and voice activity detection (VAD)

Table 1-9 describes the modes supported by the BTS 10200.

Table 1-9 Modes for Fax, Modem, and TDD Handling

Mode	Functions
T.38 Loose	Uses User Defined Protocol Transport Layer (UDPTL) packets to carry fax data; UDPTL is a UDP-based protocol not used outside of T.38 and is the most common transport for T.38. or Uses Transmission Control Protocol (TCP).
T.38 Strict	Uses UDPTL packets to carry fax data; UDPTL is a UDP-based protocol not used outside of T.38 and is the most common transport for T.38. or Uses TCP Requires remote devices (MTAs, IADs) to report their support of T.38 in the Session Description Protocol (SDP) message to the BTS 10200.
GW	Excludes CA; gateway controls how to handle calls. Always supported, even if the gateway does not do anything special for fax. Prevents CA from sending conflicting commands during gateway's special fax handling.

MGCP/NCS Interface—Fax Modes Supported

The system supports the following fax procedures from the MGCP or NCS endpoint:

- T.38 loose mode (as defined by the FXR package)
- Cisco-proprietary gateway mode (not using the FXR package)
- Fax using existing audio media (fax pass-through)—The system does not support audio codec upspeeding in this case.

SDP Attributes Support for T.38 Fax Relay

The system supports the exchange of media path (SDP or H.245) attributes between the Cisco BTS 10200 Softswitch managed end devices used to support T.38. These attributes are:

- Capabilities attributes defined in RFC-3407 (which indicate the endpoint is T.38 capable)
- T.38 attributes defined in ITU-T T.38 Annex D (which negotiates T.38 properties between endpoints)

MTA DQOS Support for T.38 Fax Relay

There are DQOS considerations for NCS MTA subscribers when switching between audio and T.38 codec. The Cisco BTS 10200 Softswitch follows the DQOS flow characteristics for T.38 sessions described in PacketCable specification “pkt-sp-codec.”

For DQOS, the Cisco BTS 10200 Softswitch creates new gates for the T.38 codec when switching to T.38 media, because endpoints can change their media IP and ports when switching between audio and T.38.

Fallback to Audio Media on T.38 Negotiation Failure

The system supports audio fallback on all interfaces supporting T.38 fax. Failure to negotiate T.38 media occurs when the non-fax detecting endpoint fails a request to modify the connection (MDCX) to T.38, and the MDCX contained a T.38 remote connection descriptor (SDP) from the fax-detecting end. When this occurs, a counter increments to track the event occurrences. Any other T.38 procedure fail scenarios do not trigger the fall back procedure. Instead, the call is cleared by the endpoint.

Audio fall back on T.38 negotiation failure requires a collaborative support by the endpoints. The MGCP/NCS endpoints requirements are:

- Non-Fax Detecting Endpoint
- Fax Detecting Endpoint

Non-Fax Detecting Endpoint

When the non-fax detecting endpoint fails the MDCX request to modify the connection to T.38, and this MDCX contained a T.38 remote connection descriptor (SDP) from the fax-detecting end, then the non-fax detecting endpoint continues with its current audio media settings.

Fax Detecting Endpoint

When the non-fax detecting endpoint fails a switch to T.38, the fax-detecting endpoint is still in T.38 media mode. The Cisco BTS 10200 Softswitch sends an MDCX to the fax detecting endpoint to abort T.38 procedures and revert back to previous audio media. The fax detecting endpoint responds with an audio SDP, and the Cisco BTS 10200 Softswitch exchanges this SDP with the remote end.

The Cisco BTS 10200 Softswitch applies the following recommendation, forecast as an update, to the MGCP FXR Package. However, it does not send the “off” Fax LCO to abort T.38 procedures. Instead, it sends an “L:<previous codec>” LCO.

For remote SIP endpoints or gateways sending a Re-Invite with T.38 SDP to switch to T.38 media receiving a fail response should fall back to previous SDP settings.

For H.323 calls, if the non-H.323 endpoint fails to switch to T.38 fax while the H.323 side is already switched to T.38 fax, then the H.323 side reapplies H.245 procedure to return to audio codec.

Audio Restore After Successful T.38 Fax Transmission

The Cisco BTS 10200 Softswitch can restore audio media after successful T.38 fax transmission. However, this feature is beyond the scope of the FXR package, and requires collaborative support by the endpoints.

For the Cisco BTS 10200 Softswitch to provide this feature, the MGCP/NCS endpoints must complete the following:

- Once the Cisco BTS 10200 Softswitch is notified of the completion of T.38 fax transmission, it sends an MDCX to the notifying endpoint to revert back to previous audio media. The notifying endpoint responds with an audio SDP, and the Cisco BTS 10200 Softswitch exchanges this SDP with the remote end.
- Remote SIP endpoints or gateways must send a Re-Invite message containing audio media SDP to restore audio.

T.38 Glare Handling

The Cisco BTS 10200 Softswitch applies a call agent controlled switch to T.38 fax media when initiated by either the originating or terminating endpoint. This includes the scenario in which both endpoints initiate the switch, causing a glare condition at the Cisco BTS 10200 Softswitch.

For details about glare handling, contact your Cisco support representative.

SDP Attributes Encoding Formats

SDP capability attributes can be formatted two ways when sent from the Cisco BTS 10200 Softswitch out of the network using MGCP, NCS and SIP protocols.

- RFC 3407 based encoding method

In this method, SDP is encoded:

```
a=sqn: 0
a=cdsc: 1 audio RTP/AVP 0 18 96
a=cpar: a=fmtp:96 0-16,32-35
       a=cdsc: 2 image udptl t38
```

- Cisco proprietary method

In this method, SDP is encoded:

```
a=X-sqn:0
a=X-cap: 1 audio 0 18 96
a=X-cpar: a=fmtp:96 0-16,32-35
a=X-cap: 2 image udptl t38
```

The Cisco BTS 10200 Softswitch selects the encoding method based on following guidelines:

- For the SIP interface, the Cisco BTS 10200 Softswitch always performs encoding using the RFC 3407-based encoding method.
- For MGCP/NCS endpoints, the Cisco BTS 10200 Softswitch uses a provisionable field to choose between the encoding methods.
- The H.323 interface does not use SDP, so this section is not applicable to H.323.

SIP Support for Call Legs

The system supports T.38 fax relay call agent controlled mode to SIP lines and trunks where one or both call legs are SIP. In addition to passing the SDP advertisement of T.38 fax codec, the Cisco BTS 10200 Softswitch issues a re-invite or similar SIP method to change the codec of an established session to a T.38 fax relay codec session once the fax event is detected (such as operating in a call agent controlled mode).

This has a dependency on SIP CPEs and media gateways. Cisco recommends that the T.38 session is initiated by the terminating side of endpoints.

For more information, refer to ITU T.38 03/2002.

Protocol Interworking

The Cisco BTS 10200 Softswitch supports T.38 for both SIP lines and SIP trunks, and interworking with the following protocols as either terminating or originating:

- MGCP line and trunk
- NCS (for cable)
- H.323 trunk

After the fax is done, the call falls back to a voice call.

The detailed protocol interworking matrix is shown in Table 1-10.

Table 1-10 Protocol interworking matrix

	H.323 Trunk	MGCP line (eMTA using NCS) and trunk	SIP line and trunk
H.323 trunk	X	X	X
MGCP (eMTA using NCS)	X	X	X
SIP line and trunk	X	X	X

Figure 1-6 shows an example of MGCP and SIP interworking.

Figure 1-6 Example of MGCP and SIP Interworking for T.38 Fax

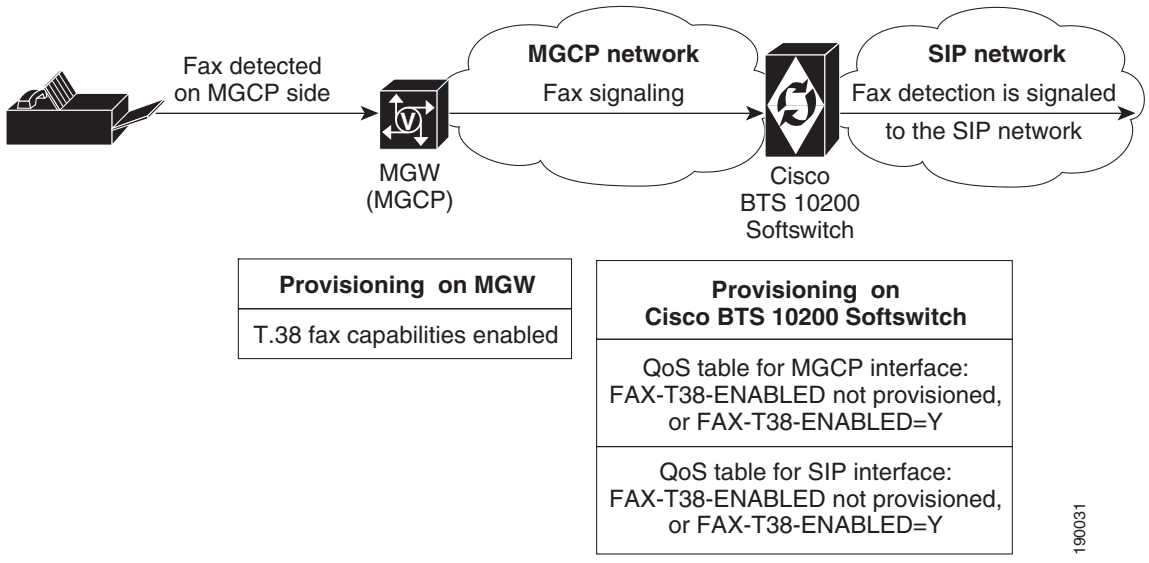


Table 1-11 illustrates how the BTS 10200 uses the T.38 fax protocol when a fax is detected. Usage depends on the value of the QoS fax_t38_enabled token for each endpoint involved in the call, as well as the protocol type of each endpoint. The symbols used in the table are:

- T38—The Cisco BTS 10200 Softswitch uses the T.38 protocol for fax transmission.
- X—The Cisco BTS 10200 Softswitch does not use the T.38 protocol for fax transmission.

- T38*—Since one of the field values in this combination is set to N, the MGCP endpoint involved in this call does not receive the local connection option (L:fxr:fx/t38) in the initial CRCX request from Cisco BTS 10200 Softswitch. However, if the endpoint receives a T.38 SDP from the remote end detecting fax, then it is assumed to support the switch to T.38 media connection.

Table 1-11 T.38 Fax Usage based on QoS Fax-t38-enabled Value

Interface/Protocol (Value)	SIP (Y)	SIP (N)	H.323 (Y)	H.323 (N)	MGCP (Y)	MGCP (N)
SIP (Y)	T38	T38	T38	X	T38	T38*
SIP (N)	T38	T38	X	X	T38*	T38*
H323 (Y)	T38	X	T38	T38	T38	X
H323 (N)	X	X	T38	T38	X	X
MGCP(Y)	T38	T38*	T38	X	T38	X
MGCP (N)	T38*	T38*	X	X	X	X

TDD Handling

Each TDD call has two call legs, one from the hearing user to the relay operator and one from the relay operator to the non-hearing user. The hearing user and the relay operator need the settings involved with a regular voice call. The non-hearing user and the relay operator need the settings that support a TDD device, so the BTS 10200 upspeeds the call between the relay operator and the non-hearing user. To provision TDD handling, set the following options in the MGW Profile table:

- TDD_TONE_SUPP to Y
- MODEM_TONE_SUPP to Y
- FAX_INBAND_METHOD to FT_UPSPEED

Control Configuration

The Cisco BTS 10200 Softswitch can be configured with either call agent controlled T.38 mode or gateway controlled T.38 mode.

Restrictions and Limitations

T.38 fax relay has the following limitations:

- Cisco BTS 10200 Softswitch Unsupported T.38 Fax Transport Methods
- Cisco BTS 10200 Softswitch Unsupported T.38 Interface
- MGCP/NCS Interface—T.38 Fax Modes Unsupported
- Relationship Between T.38 Fax Transmission and Call Features on the BTS 10200
- End-to-End SDP Exchange for T.38 Media and the H.323 Interface
- Internet Fax Terminal Endpoint Types—Not Supported
- Cisco BTS 10200 Handling of T.38 Failure Event Notification from an MGCP or NCS Endpoint

Cisco BTS 10200 Softswitch Unsupported T.38 Fax Transport Methods

The Cisco BTS 10200 Softswitch does not support following T.38 fax transport methods from ITU-T T.38:

- TCP
- Fax over RTP

Cisco BTS 10200 Softswitch Unsupported T.38 Interface

Support for ITU-T T.38 procedures are not provided on the following interfaces managed by the Cisco BTS 10200 Softswitch (including the interworking between supported and unsupported interfaces):

- H.323 subscribers.
- CAS trunks.

MGCP/NCS Interface—T.38 Fax Modes Unsupported

The Cisco BTS 10200 Softswitch does not support the following MGCP FXR package defined T.38 fax modes from the MGCP/NCS endpoint:

- Gateway mode (though the Cisco-proprietary Gateway mode is supported)
- Off mode

If the BTS 10200 does not signal any FXR fax mode in the Local Connection Options, including "Off" mode, the gateway can engage in Gateway mode. If this occurs, the BTS 10200 does not receive any Gateway mode notification events from the endpoint because it does not request them. The BTS 10200 is not notified of the gateway mode activity. The BTS 10200 honors the FXR package requirements during gateway mode by not interfering with the gateway procedures in this case.

Relationship Between T.38 Fax Transmission and Call Features on the BTS 10200

The BTS 10200 makes no distinction between calls using audio and calls using fax transmission with respect to call features.

Cisco recommends that the BTS 10200 subscribers disable the Call Waiting feature before making a call for fax transmission. This protects against any interruptions during fax transmission.

In certain multi-party call feature scenarios, such as three-way calling where a user has engaged the three-way call feature on the BTS 10200 and one party attempts a switch to T.38 fax, the endpoint fails to switch the call to T.38. The party may be either disconnected or reverted back to audio depending on the endpoints capabilities.

End-to-End SDP Exchange for T.38 Media and the H.323 Interface

The H.323 protocol must negotiate T.38 fax connection attributes (example: bit rate, maximum buffer size) during the voice call establishment using Terminal Capability Set (TCS) messages. However, for SIP and MGCP, the endpoint does not report T.38 fax connection attributes until the fax actually starts. When this occurs from an interworking H.323 endpoint to a SIP/MGCP interface, and the H.323 endpoint is ready to send TCS message during voice call establishment phase, the T.38 fax attributes are not available from the SIP/MGCP interface.

To overcome this interworking limitation, all Cisco IOS gateways assume the defaults for these attributes while exchanging TCS messages. Cisco BTS 10200 follows the same philosophy for H.323 to/from MGCP/NCS and H.323 to/from SIP calls. Cisco BTS 10200 assumes following defaults:

- Maximum Bit Rate = 14.4 kbps (This field can be configured in T38_MAX_BIT_RATE field in the CA_CONFIG table)
- Fill Bit Removal = false

- MMR Transcoding = false
- JBIG Transcoding = false
- Data Rate Management Method = transferredTCF
- Maximum Buffer Size = 200 (This field can be configured in T38_MAX_BUFFER_SIZE field in CA_CONFIG table)
- Maximum Datagram Size = 72 (This field can be configured in T38_MAX_DATAGRAM_SIZE field in the CA_CONFIG table)
- Error Correction = t38UDPRedundancy

To overcome other interworking limitations with SIP, IOS H.323 gateways send the fax UDP port in H.245 Open Logical Channel (OLC) messages. A provisioning field (REMOTE_FAX_PORT_RETRIEVAL_MSG) is added in h323-tg-profile and h323-term-profile, enabling the H.323 interface to read remote endpoint's fax UDP port either from OLC message or from OLC Ack message.

Note This does not apply to T.38 fax transmissions across H.323 to H.323 calls on the Cisco BTS 10200 Softswitch. In this case, the H.245 messages are exchanged directly through the Cisco BTS 10200 Softswitch.

Internet Fax Terminal Endpoint Types—Not Supported

The Cisco BTS 10200 Softswitch does not support endpoints that negotiate for T.38 media on initial call setup. These endpoints include internet fax terminals or internet-aware fax devices, and internet telephony gateways that only support T.38 real-time fax communications (by design or by configuration), or are statically configured to support T.38 fax calls only.

Cisco BTS 10200 Handling of T.38 Failure Event Notification from an MGCP or NCS Endpoint

The Cisco BTS 10200 Softswitch releases the call if the MGCP or NCS fax-detecting endpoint issues a "t38(failure)" event. This event is sent by the endpoint when it encounters some kind of problem with the T.38 fax relay procedure as stated in the MGCP FXR package.

Feature Provisioning Commands

To provision this feature, see the T.38 Fax Relay provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

CMTS Discovery Using the Static Subnet Table

The CMTS Discovery Using the Static Subnet Table feature uses the statically provisioned Subnet table in the BTS 10200 system. The service providers must configure all subnets handled by every CMTS using the Subnet table. The BTS 10200 uses the IP address of the multimedia terminal adapter (MTA) and the Subnet table information to determine the CMTS (AGGR) handling the MTA.

For more information on this feature and the related provisioning procedure, refer to Provisioning CMTS Discovery Using the Static Subnet Table section in the *Cisco BTS 10200 Softswitch PacketCable and Event Message Guide*.

Aggregation Id Subnet

This feature allows a service provider to use the Subnet table to statically configure all subnets handled by every Cable Modem Termination System (CMTS). The Cisco BTS 10200 Softswitch uses the IP address of the embedded Multimedia Terminal Adapter (eMTA) and Subnet table to determine the CMTS handling of a particular eMTA. An eMTA is a residential gateway. A CMTS is an aggregation device for multiple eMTAs.

An effective aggr-id is the aggr-id in effect for a particular eMTA. It identifies the CMTS to which the Cisco BTS 10200 Softswitch sends Dynamic Quality of Service (DQoS) requests for that eMTA. A manual aggr-id is an aggr-id that is provisioned by a service provider. If an aggr-id is provisioned in the Media Gateway table or Subnet table, it is a manual aggr-id.

For more information on the provisioning procedure for this feature, refer to Provisioning the Aggregation ID Subnet section in *Cisco BTS 10200 Softswitch PacketCable and Event Message Guide*.

ENUM Capability

This section describes the Cisco BTS 10200 Softswitch ENUM capability feature introduced in Release 5.0 MR1. This section specifies the feature functions and operations, and contains the following:

- ENUM Support for Routing
- ENUM Routing Use Cases
- BTS 10200 Routing Operations
- Operational Recommendations for Porting Procedures
- ENUM Clients Operation
- Planning
- Operating
- Troubleshooting

Feature Description

ENUM provides a simple query-based mechanism for applications to retrieve data associated with a particular E.164 address. The Cisco BTS 10200 Softswitch supports ENUM queries for on-net routing and LNP data. The following sections describe how the Cisco BTS supports ENUM for SIP routing and LNP queries.

ENUM Support for Routing

The ENUM Capability feature maps the called DN to the Uniform Resource Identifier (URI) to determine the switch on which the called DN resides. It then routes the call on-net. In order to use this feature, the service provider must deploy private or carrier ENUM servers that hold E.164-to-URI mapping for all DNs owned by the service provider.

Performing the ENUM Query

When receiving a call from a subscriber or from another network element, the BTS 10200 determines if it is the final destination of the call. If the BTS 10200 is not the final destination, it performs an ENUM query to determine the destination and obtains the URI to route the call.

The following rules apply to the BTS 10200 ENUM capability feature:

- The BTS 10200 launches the ENUM query after it receives the TCAP LNP query results, unless the same ENUM server is configured as LNP capable.
- The BTS 10200 does not perform ENUM queries for operator calls and casual calls.
- If the service provider does not want to perform ENUM lookup for an NPA-Nxx or wants to use different top-level domains for the ENUM queries based on a different NPA-Nxx, the BTS 10200 can be controlled on a configuration basis at the destination table level.

Routing Upon Receipt of the ENUM Response

This section describes the BTS 10200 routing operation that is based on the response from the ENUM server. In general, responses from the ENUM servers fall into two categories for routing operations:

- The BTS 10200 receives a URI indicating the final destination of the E.164 number.
- The BTS 10200 does not receive any URI information.

Call Routing Based on the Received URI

If the called DN is an on-net subscriber (that is, if it is in the VoIP domain), the ENUM server returns the URI associated with the DN, indicating the address of the destination switch that can terminate the call to the subscriber. The BTS 10200 uses the domain portion of the received URI to determine the on-net path where the call should be routed.

The BTS 10200 retrieves the domain portion from the returned URI and attempts to find the on-net route configured on the BTS 10200 (in the domain2route table). For example, if the ENUM query is launched for DN1 and the ENUM response is DN2@btsX.sp.net, the BTS 10200 ignores the DN2 and uses domain btsX.sp.net to route the call. The BTS 10200 also uses the same domain in the Req-URI field of the outgoing INVITE message (for this example, Req-URI is set to DN1@btsX.sp.net).

Because the BTS 10200 performs a longest match for the received domain with configured routes, service providers may configure only substrings in the domain2route table to keep the number of routing entries to a minimum. For example, the user can configure the BTS 10200 to use one on-net route for bts10.region1.sp.com and another for region1.sp.com (that is, all BTS 10200 nodes in region1 except BTS10).

The BTS 10200 can also specify different policy-based routing features for each domain returned from the ENUM server. For example, Percentage Based Routing and Time of Day Routing can be applied against the domain by specifying **ROUTE-TYPE = ROUTE-GUIDE**.

The user can also specify multiple routes (that is, multiple softswitch trunks) against the received domain and use the BTS 10200 Route Advance feature to select an alternate on-net route in case the first on-net route cannot be used to route the call to its final destination.

The BTS 10200 can use a destination-based route (typically pointing to the PSTN interface, such as an SS7 or SIP trunk group, toward the MGC) for a particular domain received from the ENUM server. This capability can be used in various situations, such as:

- The ENUM server returns the domain of a switch for which a direct IP route does not exist.
- There are no business arrangements for routing the call on-net between two VOIP service providers.

Finally, the BTS10200 can block the call based on the received domain. By specifying **ROUTE-TYPE=NO-ROUTE** in the domain2route table, this feature can be used in cases where information received from the ENUM server points to the domain of the BTS that launched the ENUM query.

Call Routing If the BTS Does Not Receive a URI or Receives a No Response message

If the called DN is not an on-net subscriber (is not in the VoIP domain), the ENUM server does not return a URI. The BTS 10200 performs the existing routing operation and chooses the route specified against the destination (for example, the SS7 route or the SIP route toward the MGC) to send the call towards the terminating switch.

The same behavior applies in the following situations when the BTS 10200 might not have a URI available to route the call on-net:

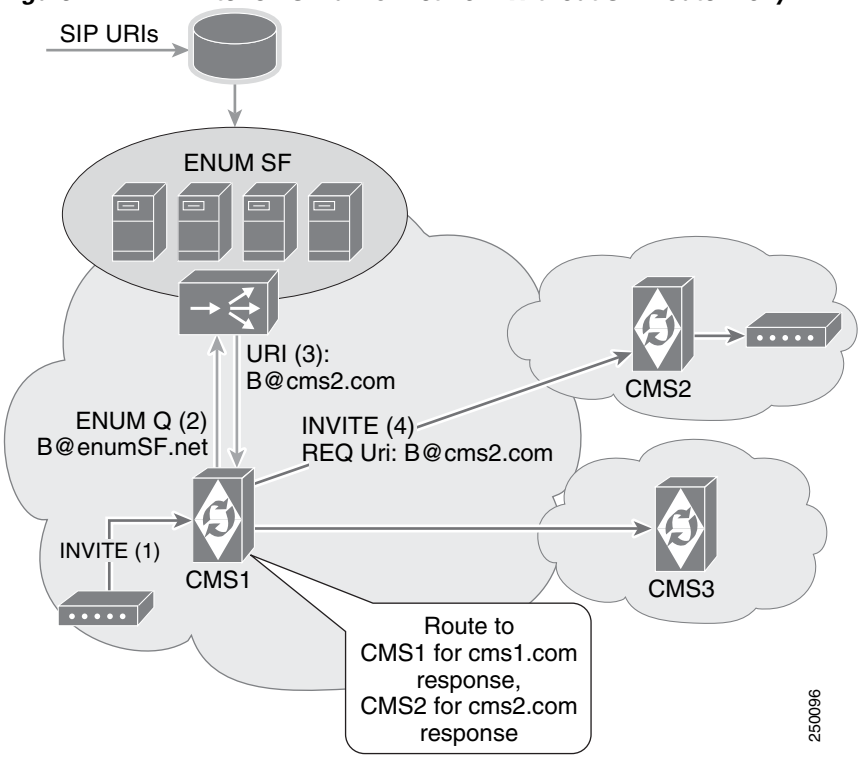
- There is no response from the ENUM server within the configured time-limit.
- No match is found for the route specified for the domain returned from the ENUM server.
- The internal BTS10200 resources are not available to perform the ENUM query.

ENUM Routing Use Cases

Selecting Inter-CMS Trunks

Figure 7 shows a typical BTS 10200 configuration for deployment to a network without a SIP route proxy. The service provider can create an inter-CMS trunk group and specify the routing policy for a particular route based on the domain portion of the return URI.

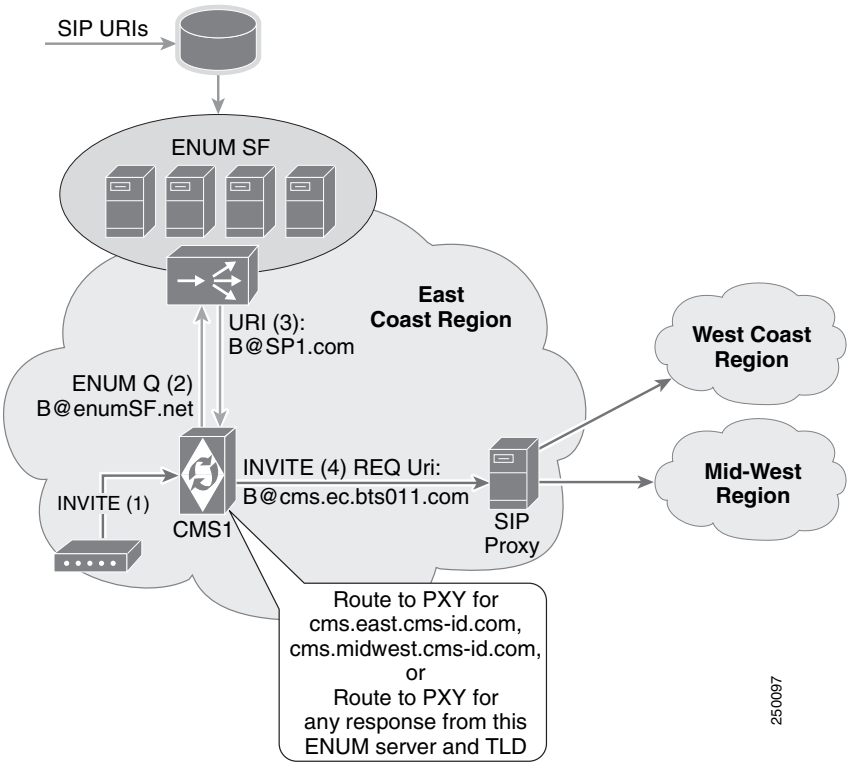
Figure 7 Inter-CMS Trunks: Network Without SIP Route Proxy



Selecting a SIP Trunk to a Route Proxy

Figure 8 shows a typical BTS 10200 configuration for deployment to a network with a SIP route proxy. The service provider can create one trunk group to go toward the SIP proxy and specify the routing logic for choosing the route, regardless of the domain of the returned URI. The domain portion of the returned URI is used in the Request URI for the outgoing SIP INVITE. The SIP proxy can direct the calls as appropriate based on this value.

Figure 8 Inter-CMS Trunks: Network With SIP Route Proxy

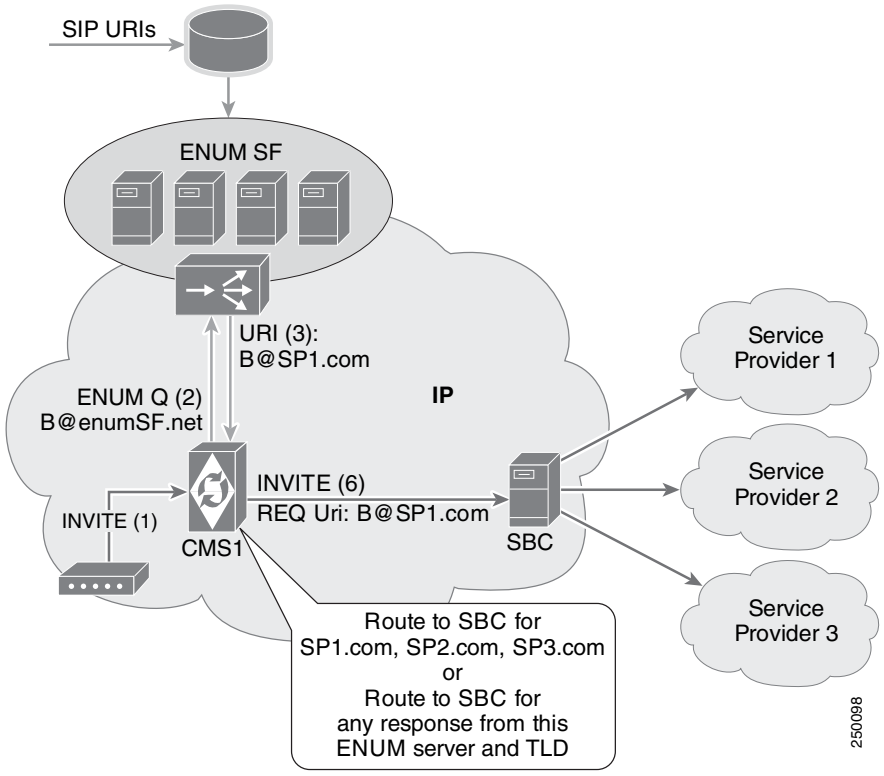


Selecting a SIP Trunk to an SBC

Figure 9 shows a typical configuration for routing calls for on-net subscribers in a different service provider domain when a peering arrangement to route on-net calls is established. A service provider typically uses a session border controller to route calls to or receive calls from a different service provider.

The service provider can direct one trunk group toward its own Session Border Controller (SBC) and specify the routing logic so it chooses a particular route, regardless of the domain in the returned URI. The domain portion of the returned URI is used in the Request URI for the outgoing SIP INVITE. The SBC can direct the calls as appropriate.

Figure 9 Routing a SIP Trunk to an SBC



ENUM Support for LNP Data

The Call Management Server (CMS) typically retrieves LNP information by sending a TCAP query toward a Signaling Control Point (SCP) database. RFC 4769 specifies another approach in which similar information can be specified in the ENUM server (E2U+PSTN NAPTR records) and retrieved through an ENUM query rather than a TCAP query. The BTS 10200 allows the user to disable the TCAP query mechanism and retrieve LNP information using the ENUM query mechanism.

The BTS 10200 retrieves the E2U+PSTN records from the ENUM server when LNP criteria match and LNP information is required.

Note The BTS 10200 will not use the domain portion specified against the rn field in the E2U+PSTN record for on-net routing described above.The BTS 10200 retrieves only the npdi flag (if available) and the user part of the rn field in the E2U+PSTN record.

BTS 10200 Routing Operations

The BTS 10200 uses the Local Routing Number (LRN) as well as the URI to make routing decisions. The following subsections describe the BTS 10200 routing. That behavior depends on information received by the BTS 10200 from the ENUM server.

BTS 10200 Receives the NPDI Indicator and LRN Information

The following table specifies the conditions that occur when the BTS 10200 receives the Number Portability Dip Indicator (NPDI) and LRN information:

If...	...Then
The URI is not available to the BTS 10200,	The BTS 10200 performs the routing operation based on the LRN. In addition, the BTS 102000 includes the NPDI indicator and LRN in the outgoing IAM/INVITE message.
The received LRN is for the same switch,	The BTS 10 2000 attempts to terminate the call to the subscriber.
The received LRN is a cluster LRN,	The BTS 10200 attempts to use the cluster dial plan routing to route the call.

BTS 10200 Receives Only Npdi Indicator

The BTS 10200 performs the routing operation based on the URI (if available) or the destination table. In addition, the BT S10200 includes the NPDI indicator in the outgoing IAM/INVITE message to indicate that the LNP query is already performed.

BTS 10200 Receives the NPDI Indicator, LRN and URI

The BTS 10200 always attempts to select SIP routes against the domain portion of the returned URI. However, if no routing policy is specified for the returned domain or the call cannot be routed on-net due to network conditions, the BTS 10200 tries to route the call based on the LRN information it received.

The user can also configure the BTS 10200 to use the ENUM functionality to retrieve LNP data but not perform domain-based routing. To do that, the user does not specify a domain-based routing policy.

Operational Recommendations for Porting Procedures

The following sections specify how customers should configure their server when a DN is ported into a VoIP network or ported out from a VoIP network.

Porting In a DN

A DN from a different network, such as a PSTN network, is ported in to the service provider network. During the transition phase

- No update is required in the LNP database.
- No update is required in the on-net routing database.

After porting is complete, the customer should do the following:

- Specify the E2U+SIP records for the ported-in number so all the switches within the VoIP network can use the on-net routing functionality.
- Update the LNP database with the LRN or cluster LRN of the destination switch to which the subscriber is ported. This information is typically used by nodes outside the VoIP domain to route the call.

Porting Out a DN

A DN from the service provider network is ported out on a switch in a different network, such as a PSTN network. During the transition phase

- No update is required in the LNP database.
- No update is required in the on-net routing database.

After porting is complete, the customer should do the following:

- Update the LNP database with the LRN or cluster LRN from the destination switch to which the subscriber is ported out.
- Remove the E2U+SIP records in the ENUM server so all VoIP nodes can use the LRN-based routing functionality.

Porting a DN to a Different Node

If a DN is moved from Node A to Node B within the same service provider network, modifying the E2U+SIP record in the ENUM server is sufficient as long as both nodes share the same LRN or cluster LRN. If the nodes have different LRNs or cluster LRNs, we recommend updating the LNP database so calls that originate in the PSTN network are efficiently routed.

ENUM Clients Operation

This section describes the processing rules for ENUM.

Launching the ENUM query

The BTS 10200 launches the ENUM query using the E.164 number of another server. The user can specify the top-level domain and predefined digits used for the query before the BTS 10200 launches the query. Use the following steps to launch the ENUM query.

Step 1 Delete from the digit string as many leading digits as specified by DEL-DIGITS in the ENUM profile, ignoring any leading or intermediate nondigit characters. For example:

digit string = 954048

DEL-DIGTS = 1

Result = 54048

Step 2 Prefix the digits specified by PFX-DIGITS in the ENUM profile to the transformed digit string after any leading nondigits or characters.

digit string = 54048

PFX-DIGITS = 1-469-25

Result = 1-469-255-4048

Step 3 Remove all nondigit characters from the transformed digit string.

digit string = 1-469-255-4048

Result = 14692554048

Step 4 Insert dots ('**.**') between the digits of the transformed digit string.

digit string = 14692554048

Result = 1.4.6.9.2.5.5.4.0.4.8

Step 5 Reverse the transformed digit string.

digit string = 1.4.6.9.2.5.5.4.0.4.8

Result = 8.4.0.4.5.5.2.9.6.4.1

Step 6 Append the ENUM domain root specified by the TOP_LEVEL_DOMAIN of the ENUM profile to the transformed digit string.

After processing is complete, the BTS 10200 sends the query to the ENUM server specified in the profile. The BTS 10200 ENUM client provides the nonblocking querying behavior to the applications

Filtering the response

After receiving the response from the ENUM server, the BTS 10200 extracts the URI used for on-net routing, according to the specifications in RFC 3761. The following steps describe how the BTS 10200 automatically filters the response.

Step 1 All NAPTR records in which the service field does not match the requested service are ignored.

Step 2 All nonterminal NAPTR records (those records in which the flags field is not u) are ignored.

Step 3 The remaining NAPTR records are sorted based on the order field (in decreasing order) and the preference field (in increasing order).

Step 4 All NAPTR records in which the regexp field contains malformed regular expressions are ignored.

Step 5 The NAPTR record at the top of the list sorted in Xref_Colorparanum is selected.

Step 6 The regular expression rules specified in the regexp field are applied to the digit string to obtain a URI.

Step 7 The required information is extracted from the URI. Any malformed URIs are ignored.

Step 8 One of the following occurs:

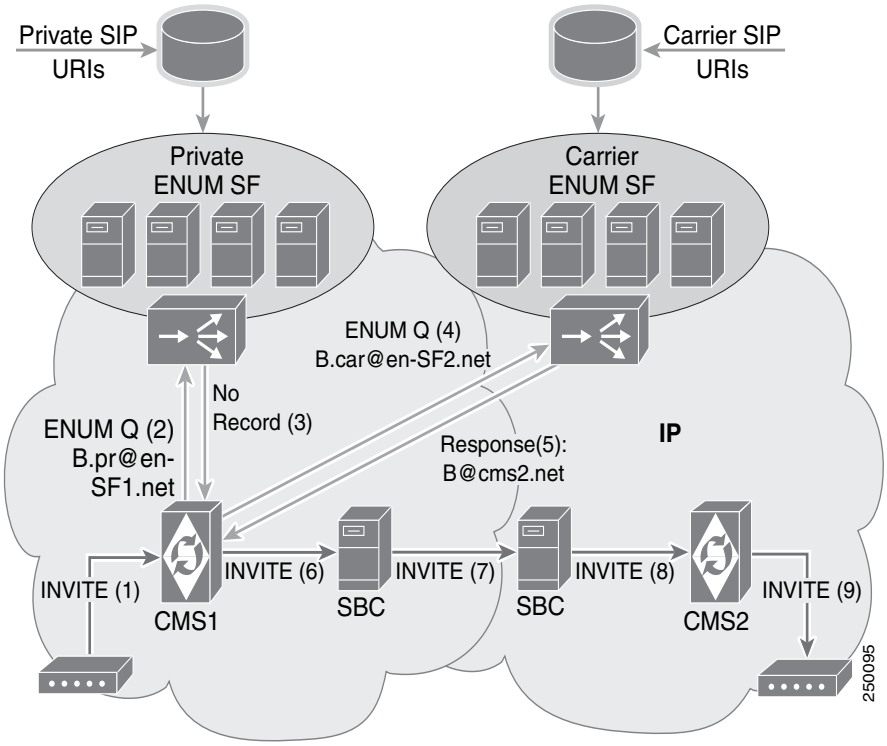
- If multiple URIs are present, the first in the list is used. Because the list has been sorted, the first in the list has priority.
- If only one URI is present, it is used for on-net routing.
- If no URIs are present, the DN is considered off-net and the call is routed using other routing rules.

Supporting Multiple Roots

The BTS 10200 can launch multiple ENUM queries toward the same set of ENUM servers or to a different set for the same call using different top-level domains. You can use this function when information for on-net subscribers is located in multiple ENUM servers, as when there is a carrier ENUM in addition to a private ENUM.

Figure 10 shows how the BTS 10200 supports multiple roots. In this example, it is configured to send an ENUM query to a private ENUM server farm. The private ENUM server farm responds with “no record found.” With the appropriate configuration, the BTS 10200 launches the query to the carrier ENUM server farm with a different top-level domain configured against the ENUM profile of carrier ENUM servers.

Figure 10 ENUM Queries for Multiple Roots



Supporting Multiple ENUM Servers

The BTS 10200 can interface with multiple ENUM servers or server farms from which it retrieves data from the SRV records. It can also distribute the ENUM queries with a round-robin or priority order policy. Refer to "Configuring the DNS" section in the *BTS 10200 Softswitch Provisioning Guide* for additional details about the selection policy. The following procedure describes how the BTS 10200 retrieves data from the SRV records.

Step 1 Send an SRV query to the default DNS server for the logical service name obtained from the ENUM_SERVER_DOMAIN field specified in the ENUM profile table.

Step 2 Obtain and compile a list of servers from the target field of each SRV record returned by the query.

Step 3 Send an A query to the default DNS server for each server obtained in the previous steps.

Step 4 Obtain and compile a list of ENUM server IP addresses associated with each server in the A records returned by the query.

The cached IP addresses are reached at predefined intervals specified in the **ENUM_SERVER_DOMAIN_TTL** field in the ENUM profile. The query retrieves all changes in network configuration or query distribution policy.

Monitoring ENUM servers and Measuring Latency

The BTS10200 uses the actual ENUM queries and test queries to monitor the status of each ENUM server. The BTS10200 sends a test query to an ENUM server if no actual ENUM queries are sent to that server during the period specified by the TEST-QUERY-INTERVAL parameter in the ENUM profile table. The test query used to monitor the status of an ENUM server is an NAPTR query.

The BTS10200 uses the following logic to update the ENUM server availability status.

- If three consecutive queries (including test queries) time-out or indicate the server is unavailable, the BTS10200 marks that ENUM server as unavailable.
- If it receives three consecutive test query responses from an ENUM server that has been marked as unavailable, the BTS10200 marks that ENUM server as available.

The BTS10200 calculates the round-trip delay for each ENUM and test query to determine the average latency associated with the ENUM server.

The BTS10200 uses the latency and availability parameters to select the ENUM server to which the next ENUM query should be sent.

Planning

This section provides information on prerequisites applicable to this feature.

Prerequisites

The service provider must deploy a private or carrier ENUM server to make use of ENUM functionality on the BTS 10200. In addition, if the ENUM LNP feature is used, the same ENUM server must be configured with E2U+PSTN records for all ported DNs.

Operating

For information on the ENUM measurements and the effect of ENUM feature on the Billing fields, refer to the *Cisco BTS 10200 Softswitch Billing Interface Guide* and the *BTS 10200 Softswitch Operations and Maintenance Guide*.

Troubleshooting

For information on ENUM signaling events and alarms, refer to *BTS 10200 Softswitch Troubleshooting Guide*.

Trunk and Line Testing

This section describes trunk and line testing features, and includes the following topics:

- Trunk Testing
- Testing Capability for 911 FGD-OS Trunks
- Network Loopback Test for NCS/MGCP Subscriber Endpoints
- Network Loopback Test for ISDN PRI Trunks

For general troubleshooting procedures, see the *Cisco BTS 10200 Softswitch Troubleshooting Guide*.

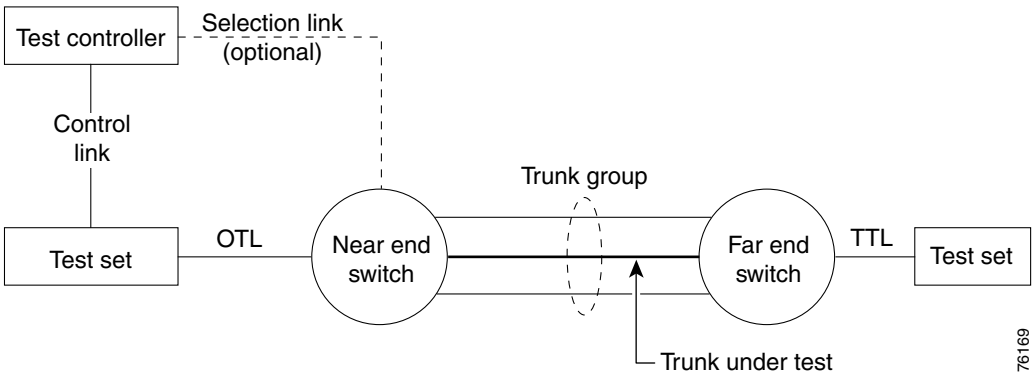
Trunk Testing

Trunk testing is used to evaluate the transmission quality of the shared trunks that interconnect switching systems. Trunk testing is extremely important in monitoring system health, because it is the only practical way to objectively evaluate the performance of individual trunks.

Trunk testing requires the following equipment and test lines. (Some additional types of equipment and lines may also be used.) A basic system setup is shown in Figure 1-11.

- Test controller
- Test set(s)
- Originating test line (OTL)
- Terminating test line (TTL)

Figure 1-11 Trunk Testing Setup



Near End Test Origination Test Calls

The BTS 10200 supports calls used to test individual trunks that connect a local gateway with a gateway or PSTN switch at a remote office. The BTS 10200 supports OTL and TTL capability. User-provided test equipment and, optionally, test controllers may be connected to the test lines. Proper selection of test equipment and test functions helps to ensure interoperability between different carriers.

The processes described in this section are applicable to the BTS 10200. The processes may work differently on other switches.

The process for testing a BTS 10200 OTL is as follows:

1. The user verifies that the remote CO has the desired 1xx test line available.
2. The user sets up a test device on a CAS TGW that is connected to the local BTS 10200.
3. The user provisions the CAS-TG-PROFILE table, setting TEST-LINE = YES. (Provisioning commands are described in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide.*)
4. On the test device at the CAS TGW side, the user enters digits representing the circuit to be tested and the test to be performed:
   - TG, for example 0003
   - Trunk number, for example 0018

   The complete trunk address in this example is 00030018.

- Test type (10x), for example 104

  The technician dials KP-00030018-104-ST.

5. The BTS 10200 automatically inserts either 9581 or 9591 in front of the test type digits to create a dialing string.

   The complete test string in this example is PREFIX | 00030018 | 9581104 | END.

   Note Alternatively, with the BTS 10200, the user can dial the test type with the 9581 or 9591 included: *KP-00030018-9581104-ST.*

6. The BTS 10200 selects the trunk to be tested based on the user-defined trunk address.
7. The TGW outpulses the digits to the remote switch over the designated trunk.

1xx Test Line Support

When the BTS 10200 is the near-end switch, the following process takes place at the remote switch:

1. The remote switch recognizes the trunk test prefix (9581 or 9591) on the incoming signal, and the test type is used to route the test to the appropriate test line.
2. The appropriate tests are performed on the test set.
3. Additional test processes may occur, depending on the specific test configuration.

When the BTS 10200 is supporting the TTL capability (test call originated at another switch), the process is as follows. The BTS 10200 receives the 958 or 959 call, recognizes the 958 or 959 type, and routes the test to the appropriate test line.

The Cisco BTS 10200 Softswitch supports the capability for a TDM-based testing device to perform continuity testing over an MF CAS TDM trunk interface. This capability requires that an MGCP-based trunking gateway is present in the test path. The TDM test type is the traditional 1xx test type, with an additional enhancement—the ability to route the test call to a specified DN on a given trunk circuit.

T108 Test Line Support

The T108 test line feature determines the performance of trunks connecting digital exchange switches, including voice over packet (VoP) softswitches. BTS 10200 incoming trunks requesting other 1xx-type test lines are routed to shared test lines for the requested tests, regardless of which gateway terminates the trunk or which gateway/IAD terminates the test line. The T108 test line feature requests a test to be performed within the same gateway where the trunk under test (TUT) is terminated, and provides a digital loopback within the gateway. The T108 test line feature supports manual and automated testing.

The T108 test line sequence is as follows:

1. The near-end switch originates the test sequence by placing a test call, identifying the trunk to be selected, and the test line number. A digital test pattern generator is used in the test setup shown in Figure 1-11.
2. The near-end switch uses the trunk identifier to override normal call processing and select only the requested trunk.
3. The far-end switch responds to the destination number and connects to the T108 test line. The T108 test line enables a digital loopback.
4. When the near-end switch receives answer supervision, it conducts digital test sequences to ascertain trunk performance.

5. Once the test sequences are completed, the near-end switch releases the test call and both switches release the trunk connection.
6. The far-end switch can detect if the test connection exceeds a preset time, and releases the test connection if the preset time is exceeded.

The T108 test line is also used for trunk redirection (wholesale dial) for Internet services where the carrier modem termination is integrated into the trunk gateway. In this case, the integral digital stored program (DSP) normally supports modem-only transmissions.

Testing Capability for 911 FGD-OS Trunks

When turning up 911 Feature Group D Operator Services (FGD-OS) trunks, there is an exchange of Off-hook/On-hook signaling and the passing of tone back and forth without a complete call setup. Signaling for this function is based on the MGCP MO package.

Upon receiving a CLI command or Test Access request, BTS 10200 sends the request to the gateway via MGCP signaling to trigger the test capability on 911 trunk at the gateway (not part of a call setup sequence). The BTS 10200 reports the result to the operator upon receiving the notification from the gateway (for example, receiving off-hook or on-hook notification). Once this gateway test capability on a 911 trunk is in place, it can be invoked remotely across the MGCP interface associated with the BTS 10200.

Note In order to support this functionality, the gateway itself must be able to provide the test capability to send and monitor the reception of the signaling and passing tone without a call setup involvement.

Network Loopback Test for NCS/MGCP Subscriber Endpoints

This feature supports the capability for a testing device to perform network loopback tests from any line-side NCS/MGCP Residential Gateway or MTA. The loopback tests can be initiated from designated test endpoints (subscribers) controlled by the BTS 10200. The procedure for setting up the test includes configuring the test lines as subscriber terminations and provisioning the MGW parameters. The system allows NCS/MGCP endpoints in a trunk group to be provisioned as a test trunk group with specific test attributes.

Restrictions and Limitations

The following restrictions and limitations apply:

- The testing and tested devices must be configured on same Call Agent. The system cannot perform network loopback test calls that originate from another switch.
- The system does not provide the ability to perform network loopback testing across H.323 or SIP networks.
- You cannot perform the Network Loopback Test if the status of the subscriber to be tested is **unequipped** (**UEQP**) or **operational-out-of-service** (**OOS**).
- Although you can test this feature using a regular MTA as the testing device by configuring the endpoints as subscriber terminations in BTS 10200, you need appropriate test equipment to perform voice-quality testing.

Configuring and Operating

The procedures for configuring the lines and gateways, and the procedure for performing the tests, are described in the Network Loopback Test section of the *Cisco BTS 10200 Softswitch Troubleshooting Guide*.

Network Loopback Test for ISDN PRI Trunks

This feature allows operators to conduct network loopback testing originating from shared ISDN PRI trunks. The shared test trunk group accepts both normal and test calls. Test calls are identified by provisioning the call-type and call-subtype tokens in the Destination table.

For detailed requirements and procedures for running this type of trunk test, see the *Cisco BTS 10200 Softswitch Troubleshooting Guide*.

CHAPTER 2

Lawful Intercept and Enhanced CALEA Features

Revised: March 24, 2011, OL-12606-21

This chapter describes the lawful intercept interface supported by the Cisco BTS 10200 Softswitch, along with enhanced CALEA features that were introduced with Release 5.0.

General Description of Lawful Intercept Implementation

The Cisco BTS 10200 Softswitch supports the call data interface and call content function for lawful intercept, along with the provisioning interface required to configure a wiretap. The BTS 10200 provides support for lawful intercept using two different, industry-developed architectures: PacketCable and the Cisco Service Independent Intercept (SII). Depending on their network type, service providers may choose to configure their networks consistent with either of these architectures in their effort to meet their obligations related to lawful intercept. Given the constantly evolving nature of industry-developed standards, service providers must recognize that the features and functionality of the BTS 10200 described below may also be subject to change over time.

Each country controls its own laws applicable to lawful intercept. For example, in the United States, one of the applicable laws is referred to as the Communications Assistance for Law Enforcement Act (CALEA).

Lawful Intercept Provisioning Interface

The BTS 10200 supports a secure provisioning interface to process wiretap requests from law enforcement agencies through a mediation device. The service provider can limit viewing and provisioning of these parameters to selected authorized personnel. The applicable parameters (entered via CLI) include the DN, tap type, and call data channel for data transmission. The tap type specifies whether the tap order is a pen register (outgoing call information), a trap and trace (incoming call information), a pen and trace (incoming and outgoing call information), or an intercept (bidirectional plus the call content).

Note To provision this feature, see the CALEA provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Lawful Intercept Call Data Interface

The BTS 10200 provides the PacketCable EMS/RADIUS interface for the transmission of call identifying information to the lawful intercept delivery function (DF) server as required by Appendix A, PCES Support, in PKT-SP-EM1.5-I02-050812, *PacketCable Event Messages Specification (EMS),* August 12, 2005.

Full call-identifying information (call data) is shipped to a DF server from the BTS 10200 for the subject under surveillance for various call types (for example, basic call and call forwarding).

Lawful Intercept Call Content Function

The call content function provides for capturing voice in a replicated Real-Time Transport Protocol (RTP) stream. The BTS 10200 can be configured to operate with simultaneous support for PacketCable intercept and Cisco SII, or with Cisco SII only.

Simultaneous support for PacketCable intercept and Cisco SII is achieved as follows: During the call-setup phase, the BTS 10200 searches for a PacketCable-compliant call-content intercept access point (IAP) in the call path. If the BTS 10200 determines that there is no such IAP available in the call path, it falls back to Cisco SII.

Note An intercept access point (IAP) is a point within a communication system where some of the communications or call identifying information of an intercept subject's equipment, facilities, and services are accessed.

Additional information about each type of intercept is provided below:

- PacketCable intercept—In PacketCable intercept, a replicated RTP stream is sent to the DF server by an aggregation router or a trunking gateway upon request from the BTS 10200. The BTS 10200 requests the relevant IAP (aggregation router or trunking gateway) to duplicate and transport the RTP stream to a predefined IP address and port number.

  The BTS 10200 uses Common Open Policy Service (COPS) protocol when sending the above request to an aggregation router, and Media Gateway Control Protocol (MGCP) when sending the request to a trunking gateway.

- Cisco Service Independent Intercept—In Cisco SII, a replicated RTP stream is sent to the DF server by an aggregation router or a trunking gateway upon request from the DF server. The DF server uses SNMPv3 as the control protocol to send the intercept request to the appropriate IAP.

Enhanced CALEA Features

This document describes enhancements to the Communications Assistance for Law Enforcement Act (CALEA) feature for the BTS 10200 Release 5.0 and contains the following sections:

- CALEA Enhancement Overview
- Generic CALEA Enhancements
- Surveillance for Calls Involving Multiple CMSs
- BTS 10200 CALEA Interaction with SIP Endpoints
- Changes to Interface between the BTS 10200 and Delivery Function Server

- BTS 10200 CALEA Interaction with SIP Triggers Feature
- CALEA Backward Compatibility
- Compliance with CALEA Requirements in PKT-SP-EM1.5-I01-050128 Appendix A
- Compliance with CALEA Requirements in PKT-SP-CMSS1.5-I01-050128 Section 7.7.2

CALEA Enhancement Overview

CALEA features were enhanced in Release 5.0 to comply with the PacketCable specifications. In addition to generic CALEA enhancements as specified in PacketCable specifications, this section includes clarifications for surveillance functions performed by the Cisco BTS 10200 when the subscriber under surveillance is configured as a SIP endpoint and when the call under surveillance involves multiple CMSs.

The CALEA feature enhancements comply with the following PacketCable specifications:

- PacketCable 1.5 Event Message Specification, PKT-SP-EM1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc. (Appendix A: EM CALEA Requirement Compliance)
- PacketCable 1.5 Call Management Server Specification, PKT-SP-CMSS1.5- I01-050128, January 28, 2005, Cable Television Laboratories, Inc. (Section 7.2.2: CMSS CALEA Requirement Compliance)

Generic CALEA Enhancements

When an origination or termination attempt is detected for a call under surveillance, the BTS 10200 issues call-data event messages to the Delivery Function device to provide call-identifying information. The BTS 10200 follows the procedural and encoding guidelines specified in PKT-SP-EM1.5-I01-050128 Appendix A for sending these event messages. Table 2-1 lists all the call-data event messages supported by the BTS 10200.

Table 2-1 CALEA Call-Data Event Messages Supported by the BTS 10200

Message	Description
Signaling Start	The BTS 10200 generates this message whenever an origination attempt or termination attempt is detected for a call under surveillance.
Media Report	The BTS 10200 generates this message when SDP information from both sides of the call is available for the call under surveillance.
Call Answer	The BTS 10200 generates this message whenever a call under surveillance moves to the answered state.
Call Disconnect	The BTS 10200 generates this message whenever a call under surveillance moves to the disconnected state.
Signaling Stop	The BTS 10200 generates this message when a call under surveillance has ended.

Table 2-1 CALEA Call-Data Event Messages Supported by the BTS 10200 (continued)

Message	Description
Service Instance	The BTS 10200 generates this message when a feature is invoked by the BTS 10200 for the subject under surveillance. **Note** The BTS 10200 does not send this message if it is not aware of a service invocation (for example, a Call Waiting at a SIP endpoint).
Signal Instance	The BTS 10200 generates this message whenever it receives information from the subject or sends information to the subject. **Note** The BTS 10200 cannot (and is not required to) report some signals if the tapped user has a SIP endpoint (refer to Table 2-3 for detailed information) or for cases in which the BTS10200 does not apply the signal itself to NCS endpoints. For example, the Ringback signal is not applied and not reported to the DF if the media-gateway of the terminating party (C) is able to provide the remote ringback. **Note** This message is new in Release 5.0.
Redirection	The BTS 10200 generates this message if call forwarding/transfer is invoked by the BTS 10200 for the associate of the subscriber under surveillance. **Note** This message is new in Release 5.0.
Surveillance Stop	The BTS 10200 generates this message when the surveillance function for a call under surveillance ends. **Note** This message is new in Release 5.0.
Conference Party Change	The BTS 10200 generates this message if the subscriber under surveillance joins two calls (using the Three-way call feature on BTS) and if one of the communicating parties subsequently leaves the conference. **Note** The BTS 10200 does not send this message if it is not aware of the three-way call (for example, a three-way call at a SIP endpoint). **Note** This message is new in Release 5.0.

Detailed information about compliance with the requirements in specification PKT-SP-EM1.5-I01-050128 Appendix A is provided in Table 2-4.

Surveillance for Calls Involving Multiple CMSs

When a call under surveillance spans multiple call management systems (CMSs), one CMS might not have access to all call identifying information or call-content intercept-access points to perform surveillance. RFC-3603 and PKT-SP-CMSS1.5- I01-050128 specify the procedure for a CMS to request other adjacent CMSs to perform surveillance on its behalf. According to these procedures, a CMS can request a CMST (CMS at the terminating side of the call) or a CMST (CMS at the originating side of the call) to perform surveillance functions. The CMS uses the SIP P-DCS-LAES header to make the request.

The Cisco BTS 10200 supports the sending and receiving of the P-DCS-LAES header in various SIP messages using guidelines specified in PacketCable specification PKT-SP-CMSS1.5- I01-050128. The detailed compliance with the procedures specified in the PKT-SP-CMSS1.5- I01-050128 specification is provided in Table 3. The following statements describe how the Cisco BTS 10200 uses the SIP P-DCS-LAES header to implement CALEA.

- When the BTS 10200 requires assistance from another CMS to perform the call-data surveillance function or call-data and call-content surveillance function, it includes the SIP P-DCS-LAES header in a SIP message. Depending on the call scenario, the following SIP messages can carry the P-DCS-LAES header as an indication of a surveillance request sent to the CMST or CMS:
  - INVITE (or RE-INVITE) message
  - 183 Progress
  - 180 Alerting
  - 200 OK
  - 302 Redirection
- When the BTS 10200 requires the assistance of an adjacent CMS in performing the call-data surveillance function, it includes BCID, CDC-IP-Address, and CDC-IP-Port information in the SIP P-DCS-LAES header.
- When the BTS 10200 requires the assistance of an adjacent CMS to perform the call-data and call-content surveillance functions, it includes BCID, CDC-IP-Address, CDC-IP-Port, CCC-ID, CCC-IP-Address, and CCC-IP-Port information in the SIP P-DCS-LAES header.
- When the BTS 10200 receives P-DCS-LAES header information in any of the following SIP messages, it takes on the surveillance responsibility based on the content of SIP P-DCS-LAES header.
  - The BTS 10200 assumes the responsibility of Call-Data surveillance if the P-DCS-LAES header is included in a SIP message with valid BCID, CDC-IP-Address, and CDC-IP-Port information.
  - The BTS 10200 assumes the responsibility of Call-Data and Call-Content if the P-DCS-LAES header is included in a SIP message with BCID, CDC-IP-Address, CDC-IP-Port, CCC-ID, CCC-IP-Address, and CCC-IP-Port information.

  The grammar for the P-DCS-LAES header is specified in two documents: PKT-SP-CMSS1.5-I01-050128 Section 7.7.2.1 and RFC 3603 Section 8. The BTS 10200 conforms to the grammar rules specified in PKT-SP-CMSS1.5-I01-050128 Section 7.7.2.1 for the encoding and decoding of the P-DCS-LAES header.

P-DCS-Redirect = “P-DCS-Redirect” HCOLON Called-ID *(SEMI redir-params)

Called-ID = LDQUOT addr-spec RDQUOT

redir-params = redir-uri-param / redir-count-param /generic-param

redir-uri-param = “redirector-uri” EQUAL Redirector

Redirector = LDQUOT addr-spec RDQUOT

redir-count-param = “count” EQUAL Redir-count

Redir-count = 1*DIGIT

BTS 10200 CALEA Interaction with SIP Endpoints

The BTS 10200 Softswitch follows the guidelines specified in PKT-SP-EM1.5- I01-050128 Appendix A for sending call-identifying information to the delivery function for SIP endpoints. While attempting to deliver call-content information, the BTS 10200 notifies the DF server about the unavailability of call-content IAP on either the originating side or terminating side of the call. These packet-cable compliant call-content IAPs typically are not available when the caller and called are SIP endpoints. In order to capture call-content information for these cases, the Delivery Function Server must use the Service Independent Intercept (SII) architecture and initiate a request for duplication of RTP streams.

Note the following additional clarifications about satisfying CALEA requirements for SIP endpoints:

- If feature functionality is provided at the endpoint, the BTS 10200 does not receive any explicit indication about the feature provided by the endpoint. Therefore the BTS 10200 is not required to send Service Instance messages indicating invocation of a feature.
- The requirements in PKT-SP-EM1.5- I01-050128 Appendix A that pertain to sending Signal Instance messages is explicitly designed for NCS/MGCP endpoints. If a tapped subscriber is using SIP endpoints, the BTS 10200 does not instruct the endpoint to play any signals/tones towards the user explicitly. However, the BTS 10200 may send information in SIP messages that trigger an endpoint to play tone or display information to the user. Table 2-2 defines how the BTS10200 behaves with regard to sending Signal Instance messages when a tapped subscriber is using a SIP endpoint.

Table 2-2 Signals Supported for Signaling Instance Messages to SIP Endpoints

Signal Type	BTS 10200 Behavior
Busy Tone	BTS10200 reports SIGNAL INSTANCE message with Audible tone = BUSY when it sends a 486 busy towards the SIP endpoint under surveillance.
Calling Name/Number	BTS10200 reports SIGNAL INSTANCE message with Terminal Display attribute containing Calling Name, Calling Number, and Date if they are included in the INVITE message sent toward the subject with SIP endpoint.
Ringing Tone	BTS10200 reports SIGNAL INSTANCE message with Audible signal = ringing when it receives a 180 Alerting from the subject with SIP endpoint. **Note** In this case, the SIP Endpoint might have played a call-waiting tone instead towards the user.
Distinctive Ringing Tone	BTS10200 reports SIGNAL INSTANCE message with Audible signal = distinctive ringing when it receives a 180 Alerting from the subject with SIP endpoint and the BTS10200 included the Alert-Info header in the SIP INVITE message sent towards the user. **Note** In this case, the SIP Endpoint might have played a call-waiting tone or a normal ringing tone instead towards the user.
Ring back tone	BTS10200 reports SIGNAL INSTANCE message with Audible signal = ringing after sending an 180 Alerting to the subject with SIP endpoint.

Table 2-2 Signals Supported for Signaling Instance Messages to SIP Endpoints (continued)

Signal Type	BTS 10200 Behavior
Reorder tone	BTS 10200 reports SIGNAL INSTANCE message with Audible signal = reorder-tone when it receives an INVITE message that is processed but cannot be routed due to reasons such as Invalid destination number, routing failure, etc. The BTS 10200 typically sends a 4XX or 5XX message to the SIP endpoint in such scenarios.
Message Waiting indicator/ Visual Message waiting indicator	BTS10200 reports SIGNAL INSTANCE message with Terminal Display Attribute = VMWI_ON or VMWI_OFF. **Note** Instead, the SIP Endpoint might play a Message waiting indicator tone towards the subject instead of providing a VMWI signal.

Table 2-3 specifies the SIGNALS that are not reported by BTS10200 when a tapped user is associated with a SIP endpoint.

Table 2-3 Unsupported Signals for Signaling Instance Messages to SIP Endpoints

Signal Type	BTS 10200 Behavior
Stutter Dial tone	BTS10200 does not request the SIP endpoint to play a Stutter Dial tone.
Confirmation Tone	BTS10200 does not request thee SIP endpoint to play a confirmation tone.
Dial tone	BTS10200 does not request the SIP endpoint to play Dial tone.
Off-hook warning tone	BTS10200 does not request SIP endpoint to play off-hook warning tone. Endpoint may decide to play this tone depending on its own capability or configuration.
Ring Splash	BTS10200 does not request the SIP endpoint to play a Ring splash.
DTMF tones	BTS10200 does not send out-of-band DTMF signals towards SIP endpoints.
Call Waiting tone	BTS10200 cannot detect when a SIP endpoint plays a call-waiting tone towards the user interface. Call Waiting tone is a SIP endpoint feature.

Changes to Interface between the BTS 10200 and Delivery Function Server

This section summarizes how the message interface between the BTS 10200 and the Delivery Function server differs from the preceding BTS 10200 release.

- The BTS 10200 Release 5.0 implements the following additional messages along with the associated attributes to deliver call-identifying information towards the Delivery function server. The details of the message and associated attributes are provided in PKT-SP-EM 1.5-101-050128, Appendix A.
  - Signal Instance
  - Redirection
  - Surveillance Stop

  - Conference Party Change

- The BTS 10200 Release 5.0 also implements the Electronic Surveillance Indication attribute in the Signaling Start message as defined in PKT-SP-EM 1.5-101-050128, Appendix A. However, this attribute can be used in many call scenarios other than those explicitly presented in packet-cable specifications. The BTS 10200 implements this attribute according to the following guidelines:
  - The BTS 10200 includes the Electronic Surveillance Indication attribute in a Signaling Start message sent from the forwarded-to party in case the call was already under surveillance as a result of a wiretap on the party forwarding the call.
  - The BTS 10200 includes the Electronic Surveillance Indication attribute in a Signaling Start message sent from the final terminating party in case surveillance responsibility is transferred to the BTS from other parties involved in the call due to their inability to perform complete surveillance.
  - The BTS 10200 includes the Electronic Surveillance Indication attribute in a Signaling Start message sent from an originating party in case surveillance responsibility is transferred to the BTS from other parties involved in the call due to their inability to perform complete surveillance.
- The message flows between the BTS 10200 and the Delivery Function server have changed for call-forwarding and call-redirection cases since the preceding release. The changes ensure that a common logic can be used at the Delivery Function server without regard to the number of CMSs and the number of taps involved in the call path. The following case shows the changes to the interface between the BTS 10200 and delivery function server.

Scenario Example

A@cms1 calls B@cms1. B@cms1 has an active call-forwarding unconditional feature to forward all calls to C@cms1. B is the tapped party in this call scenario.

The BTS 10200 Release 4.5 implementation uses the following messages to send call-identifying information to the Delivery Function server:

—> DF (BCID-Bt) Signaling Start (Terminating) (Calling: A) (Called: B)

—> DF (BCID-Bo) Signaling Start (Originating) (Calling: A) (Called: C) (ESI Remote-BCID: (BCID-Bt))

—> DF (BCID-Bo) Service Instance (Call Forward) (Related-BCID: BCID-Bt) (Redirected-From: B) (Redirected-To: C)

—> DF (BCID-Bo) Media Report (Open) (CCCID: X)

—> DF (BCID-Bo) Call Answer (Charge Number: B)

---------- Active Call under surveillance ----------

—> DF (BCID-Bo) Media Report (Close) (CCCID: X)

—> DF (BCID-Bo) Call Disconnect

—> DF (BCID-Bo) Signaling Stop

—> DF (BCID-Bt) Signaling Stop

The BTS 10200 Release 5.0 implementation uses the following messages to send call-identifying information to the Delivery function server:

—> DF (BCID-Bt) Signaling Start (Terminating) (Calling: A) (Called: B)

—> DF (BCID-Bo) Signaling Start (Originating) (Calling: A) (Called: C) (ESI Remote-BCID: (BCID-Bt))

—> DF (BCID-Bt) Signal Instance (Network Signal) (rs) (Signal-To-Party: B)

—> DF (BCID-Ct) Signaling Start (Terminating) (Calling: A) (Called: C) (ESI Remote-BCID: (BCID-Bo))

—> DF (BCID-Bo) Service Instance (Call Forward) (Related-BCID: BCID-Bt) (Redirected-From: B) (Redirected-To: C)

—> DF (BCID-Ct) Media Report (Open) (CCCID: X)

—> DF (BCID-Ct) Signal Instance (Network Signal) (rg) (Signal-To-Party: C)

—> DF (BCID-Ct) Call Answer (Charge Number: B)

---------- Active Call under surveillance ----------

—> DF (BCID-Bt) Signaling Stop

—> DF (BCID-Ct) Media Report (Close) (CCCID: X)

—> DF (BCID-Bo) Signaling Stop

—> DF (BCID-Ct) Call Disconnect

—> DF (BCID-Ct) Signaling Stop

—> DF (BCID-Ct) Surveillance Stop (End of Surveillance)

BTS 10200 CALEA Interaction with SIP Triggers Feature

To use the SIP triggers feature functionality (not defined by the PacketCable 1.5 specifications) on the BTS 10200, a call can be routed to an external application server for feature processing. The BTS 10200 supports two types of triggers: Originating Trigger and Terminating Trigger. For both types, when a trigger is detected, the BTS 10200 routes the call to the application server through a SIP interface. Typically, the application server executes the feature logic and performs one of the following two operations to enable the BTS 10200 to route the call to the final destination.

- An application server might initiate a new call (by sending a new INVITE message) to the BTS 10200 and include a SIP header to enable the BTS 10200 to associate the new call with the original call for which feature logic was invoked.
- An application server might send a 3XX redirect back to the BTS 10200 when feature logic processing is complete.

The rest of this section summarizes how the BTS 10200 operates and interacts with the application server to perform surveillance on calls for which the Originating or Terminating Trigger feature is invoked.

When the BTS 10200 detects any origination or termination attempt, it checks for active surveillance associated with the originating or terminating party before routing the call to the application server. If the subscriber is under surveillance, the BTS 10200 sends a Signaling Start message to the Delivery Function server and performs the call-content surveillance function on an available call-content Intercept access point. In addition, when the call is being routed to the application server, the BTS 10200:

- Initiates a new Signaling Start message with Electronic Surveillance Indication attribute containing the billing-correlation-id set to the billing-correlation-id included in the previous Signaling Start message sent to the Delivery Function server.

- Includes a P-DCS-LAES header with a billing-correlation-id associated with the terminating half of the call.

If the application server redirects the call-back to the BTS 10200, the BTS 10200 forwards the surveillance to the terminating side of the call. However, if the application server initiates a new call (by sending new INVITE message) to the BTS 10200, the BTS 10200 expects the same (unchanged) P-DCS-LAES header (sent earlier on the original call) in the new INVITE message. The BTS 10200 performs the following operations when it receives an INVITE message from the application server:

- Initiates a new Signaling Start message with Electronic Surveillance Indication attribute containing the billing-correlation-id set to the billing-correlation-id included in the previous Signaling Start message sent to the Delivery Function server
- Transfers the surveillance towards the terminating side of the call

In addition, if the surveillance function cannot be performed on the terminating side of the call, the BTS 10200 includes a new P-DCS-LAES header in an 18X or 200 response sent back to the application server. It is assumed that the application server can include the P-DCS-LAES header in a SIP Response message sent back to the BTS 10200 on the original call.

CALEA Backward Compatibility

The Enhanced CALEA feature in Cisco BTS 10200 Release 5.0 implements new messages and attributes defined in newer versions of the PacketCable specifications. In addition, the BTS 10200 has enhanced the internal algorithms to select the call-content IAPs according to the requirements associated with support of the P-DCS-LAES header for performing the surveillance function across multiple CMSs. These enhancements required additional development in the Delivery Function server so that it could continue performing surveillance functions for call-scenarios that include a single CMS or multiple CMSs. For a case in which the event Enhanced Delivery function server is not available, the BTS 10200 provides configuration options (EM-PROTOCOL-VERSION-MAJOR and EM-PROTOCOL-VERSION-MINOR flags in the ESS table) which enable the BTS to interoperate with existing software versions of the Delivery Function server.

Note By using the configuration options, the BTS 10200 provides backward compatibility by disabling the new messages and attributes implemented in BTS10200 Release 5.0. However, BTS 10200 Release 5.0 does not provide backward compatibility to permit selecting the call-content IAP to generate the duplicate call-content based on the algorithm implemented in older releases of the BTS 10200 software.

Note The BTS 10200 enables use of the version flags that provide backward compatibility for certain requirements (or implementations) to avoid interoperation problems with the current version of the Delivery Function server. However, the BTS 10200 does *not* provide control for *all* of the different versions of the PacketCable specifications that describe the use of these flags.

CALEA Operation Similar to BTS Release 4.5

To configure CALEA to operate as it did for BTS 10200 Release 4.5, set the following ESS table tokens as follows:

Option 1

- EM-PROTOCOL-VERSION-MAJOR = 11

- EM-PROTOCOL-VERSION-MINOR = 06
- GENERAL-PURPOSEFLAG = 1

In this configuration, the BTS 10200 does not send the P-DCS-LAES header and ignores the receipt of the P-DCS-LAES header. The BTS also disables support of all the new messages implemented on top of BTS 10200 Release 4.5 (which include, SIGNAL INSTANCE, REDIRECTION, CONFERENCE PARTY CHANGE, SURVEILLANCE STOP). Furthermore, the BTS disables the Electronic Surveillance Indication attribute in the Signaling Start message. In addition, the BTS 10200 does not attempt to forward the surveillance responsibility towards the terminating party in call-forwarding situations, assuming that the forwarding party remains in the call path for the duration of the call.

For this option, set the following Softswitch Trunk Group Profile table tokens as follows:

- ENABLE_P_DCS_LAES_HEADER = N
- SEND_LAES_IN_RESPONSE = N
- ENABLE_ES_EVENTS = N

CALEA Operation Similar to BTS Release 4.5 with SIGNAL INSTANCE Message

To configure CALEA to operate as it did for BTS 10200 Release 4.5, with the addition of SIGNAL INSTANCE MESSAGE support, set the following ESS table tokens as follows:

Option 2:

- EM-PROTOCOL-VERSION-MAJOR = 11
- EM-PROTOCOL-VERSION-MINOR = 07
- GENERAL-PURPOSEFLAG = 1

In this configuration, the BTS 10200 does not send the P-DCS-LAES header and ignores the receipt of the P-DCS-LAES header. The BTS also disables the sending of all the new messages defined only in PacketCable 1.5 specifications (which include, REDIRECTION, CONFERENCE PARTY CHANGE, SURVEILLANCE STOP). The BTS also disables the Electronic Surveillance Indication attribute in the Signaling Start message. Furthermore, the BTS 10200 does not attempt to forward the surveillance responsibility towards the terminating party in call-forwarding situations, assuming that the forwarding party remains in the call path for the duration of the call.

For this option, set the following Softswitch Trunk Group Profile table tokens as follows:

- ENABLE_P_DCS_LAES_HEADER = N
- SEND_LAES_IN_RESPONSE = N
- ENABLE_ES_EVENTS = N

CALEA Operation According to PacketCable 1.5 Specification

To configure the CALEA feature to operate according to the PacketCable 1.5 specifications, set the following ESS table tokens as follows:

Option 3:

- EM-PROTOCOL-VERSION-MAJOR = 11
- EM-PROTOCOL-VERSION-MINOR = 07
- GENERAL-PURPOSEFLAG = 0

In this configuration, the BTS 10200 sends the P-DCS-LAES header and processes the receipt of the P-DCS-LAES header based on configuration options specified by various flags in the Softswitch Trunk Group Profile (softsw-tg-profile) table. The BTS also supports of all the new messages defined only in Packet-cable 1.5 specifications (which include, REDIRECTION, CONFERENCE PARTY CHANGE, SURVEILLANCE STOP). The BTS also enables support of the Electronic Surveillance Indication attribute in the Signaling Start message. Furthermore, the BTS 10200 forwards the surveillance responsibility towards the terminating party in call-forwarding/transfer situations.

Compliance with CALEA Requirements in PKT-SP-EM1.5-I01-050128 Appendix A

Table 2-4 describes the requirements included in the PacketCable specification PKT-SP-EM1.5-I01-050128, Appendix A and indicates the level of compliance provided by the CALEA feature in Cisco BTS 10200, Release 5.0.

Note If the endpoint type is a SIP endpoint, refer to Table 2-1. The section "BTS 10200 CALEA Interaction with SIP Endpoints" section on page 2-6 identifies caveats that pertain to the operation of CALEA with SIP endpoints.

Table 2-4 Cisco BTS 10200 Release 5.0 Compliance with PKT-SP-EM 1.5-101-050128, Appendix A

Requirement	Description	Compliance
REQ2529	The PCES event message sent to the delivery function (DF) must not affect the monotonically increasing sequence-number that appears in the Event Message header sent to the RKS.	Compliant
REQ6108	All PCES event messages must have the Event Object field in the EM Header attribute set to 1.	Compliant
REQ6109	PCES event messages must not be sent to the RKS.	Compliant
REQ6110	Intercept Access Points (for example, CMS, CMTS, and MGC) and DF must support the Radius Protocol over UDP.	Compliant
REQ6111 REQ6112	If an IAP does not receive an Accounting-Response message within the configured retry interval, it must continue resending the same Accounting-Request until it receives an acknowledgment from the DF or the maximum number of retries is reached. The IAP can drop the request after the maximum retries is reached.	Compliant
REQ6113	When a DF receives a PCES event message in a Radius Accounting-Request message from an IAP, it must send an Accounting-Response message to the IAP.	Not applicable
Section A.1, Service Instance Message		
REQ2530	If the service (call) is under surveillance, the Service Instance Event Message must be generated with all the standard required parameters and with the additional required electronic surveillance parameters.	Compliant
Section A.2, Signaling Start		
REQ2534	If the service is under surveillance as defined in requirement 8, this event message must be generated with all the standard required parameters and with the additional required electronic surveillance parameters.	Compliant

Table 2-4 Cisco BTS 10200 Release 5.0 Compliance with PKT-SP-EM 1.5-101-050128, Appendix A (continued)

Requirement	Description	Compliance
REQ2535	The MGC must generate, timestamp, and send this event to the DF for a terminating call under surveillance to a PSTN gateway.	Compliant
REQ2536	The MGC must timestamp this message when it sends the SS7 IAM message or transmits the dialed digits on an MF-trunk.	Compliant
REQ2537 REQ2538	For an originating call from an MTA or from a PSTN Gateway, if the MGC receives signaling notification from the terminating CMS that the call is to be intercepted but the terminating device is unable to perform the interception, the MGC must timestamp and send an additional Signaling_Start event message to the Electronic Surveillance Delivery Function before it delivers a response to the originating MTA or PSTN gateway. This Signaling_Start event message must contain the Electronic_Surveillance_Indication attribute, and the value of the Direction_Indicator attribute must be integer 2 (2=Terminating).	Compliant
REQ2539	The CMS must generate, timestamp, and send this event to the DF if the originating call from an MTA is under surveillance.	Compliant
REQ2540	The CMS must timestamp and send this event message to the DF after all translation of the dialed digits is complete, whether the translation is successful or not. This includes unroutable digits reported to the CMS (that is, partially dialed digits).	Compliant
REQ2541	The CMS must generate, timestamp, and send this event to the DF for a terminating call to an MTA under surveillance, or for a terminating call under surveillance to an MTA.	Compliant
REQ2542	The CMS must timestamp and send this event message to the Electronic Surveillance Delivery Function prior to invoking any termination features.	Compliant
REQ2534.13.1	The Electronic_Surveillance_Indication attribute must be present in events sent to the DF for terminating calls that have been redirected by a surveillance subject.	Compliant
Section A.3, Signaling Stop		
REQ6120	If the service (call) is under surveillance, this event message must be generated with all the standard required parameters and with the additional required electronic surveillance parameters.	Compliant
REQ6121	A Signaling_Stop message must not be generated unless a Signaling_Start message with the same BCID has been generated for the call.	Compliant
REQ6122	A Signaling_Stop message *must* be generated if a Signaling_Start message with the same BCID has been generated for the call (In exception cases, this may be the result of a proprietary timeout or cleanup process.)	Compliant
REQ6123	Originating CMS: In the single-zone scenario, the originating CMS must timestamp this EM message immediately upon transmission of the NCS-signaling DLCX message.	Compliant
REQ6124	Originating CMS: In the intradomain or interdomain scenario, the originating CMS must timestamp this message upon transmission of the last signaling event in the following list: • Transmission of the NCS-signaling DLCX message • Transmission of the CMSS-signaling BYE message or CANCEL message	Compliant
REQ6125	Terminating CMS: In the single-zone scenario, the terminating CMS must timestamp this EM message immediately upon transmission of the NCS-signaling DLCX message.	Compliant

Table 2-4 Cisco BTS 10200 Release 5.0 Compliance with PKT-SP-EM 1.5-101-050128, Appendix A (continued)

Requirement	Description	Compliance
REQ6124	Terminating CMS: In the intradomain or interdomain scenario, the originating CMS must timestamp this message upon transmission of the last signaling event in the following list: • Transmission of the NCS-signaling DLCX message • Transmission of the CMSS-signaling BYE message or CANCEL message	Compliant
REQ6124	Originating MGC (off-net to on-net): The originating MGC must timestamp this EM message immediately upon the last signaling event in the following list: • REQ6127.1—Transmission/receipt of an RLC to/from the Signaling Gateway that communicates with the SS7 network • REQ6127.2—Transmission of the MGC-issued TGCP DLCX message • REQ6127.3—Receipt of an MG-issued TGCP DLCX message • REQ6127.4—Transmission of the CMSS-signaling BYE message or CANCEL message	Compliant
REQ6128	Terminating MGC (on-net to off-net). The terminating MGC must timestamp this EM message immediately upon transmission of the TGCP-signaling DLCX message.	Compliant
Section A.4, Call Answer		
REQ2552	If the service (call) is under surveillance, this event message must be generated with all the standard required parameters and with the additional required electronic surveillance parameters.	Compliant
REQ2553	The CMS or MGC must send this event message to the DF.	Compliant
Section A.5, Call Disconnect		
REQ2556	If the service (call) is under surveillance, this event message must be generated with all the standard required parameters and with the additional required electronic surveillance parameters.	Compliant
REQ2557	The CMS or MGC must send this event message to the DF.	Compliant
	Section A.6, QOS Reserve (Not applicable)	
	Section A.7, QOS Releases (Not applicable)	
	Section A.8, QOS Commit (Not applicable)	
Section A.9, Media Report Message		
REQ5992	The CMS and MGC must send this message: REQ5992.1—When it opens a new media channel and receives a confirmation that include identification of the Session Description Protocol (SDP) REQ5992.2—When it closes a media channel REQ5992.3—When it receives a new SDP for an open media channel	Compliant
REQ5993	REQ5993—The CMS or MGC must timestamp this message on receipt of response from an endpoint that triggered the sending of the message (for example, a response from a modify or delete connection).	Compliant
REQ6071	REQ6071.1—The EM_Header attribute must be present as the first attribute of the EM.	Compliant

Table 2-4 Cisco BTS 10200 Release 5.0 Compliance with PKT-SP-EM 1.5-101-050128, Appendix A (continued)

Requirement	Description	Compliance
REQ6001	REQ6001.1—The CCC_ID attribute must be present for call content surveillance. CMS and MGC provide CCC_ID. REQ6001.2—The CCC_ID attribute must not be present for call data surveillance.	Compliant
REQ6002	REQ6002.1—The SDP_Upstream attribute must be included if SDP is received from the surveillance subject's associate.	Compliant
REQ6003	REQ6003.1—The SDP_Downstream attribute must be included if SDP is received from the surveillance subject.	Compliant
REQ6072	REQ6072.1—The Channel_State attribute must be included and set to "Open" if a new channel has been opened, to "Change" if SDP is being provided for an opened channel, or to "Close" if the media channel has been closed.	Compliant
REQ6073	REQ6073.1—The Flow_Direction attribute must be included and it must indicate the direction of flow, either upstream or downstream.	Not Compliant (BTS includes both SDPs in one Media report message.)
Section A.10, Signal Instance Message Section A.11, Terminal Display Information Attribute Structure		
REQ5994	If the service is under surveillance, the Signal Instance message must be generated and time-stamped when any of the following events occurs, unless the information reported in the Signal Instance message would be redundant with the information reported by other event messages (for example, Signaling_Start): • REQ5994.1—The CMS receives a positive acknowledgment in response to a Notification Request command that asked for immediate generation of a signal contained in Table 66 the surveillance subject • REQ5994.2—The CMS receives a Notify command that indicates the surveillance subject's initiation of a signal contained in Table 67 of the PacketCable specification. • REQ5994.3—For DTMF tones, the CMS must not generate the Signal Instance message until it has received all of the digits provided by the surveillance subject.	Compliant
REQ5997	When the generation of the Signal Instance message is due to Condition 1 in the preceding requirement (REQ5994), the Signal_Type attribute in Table 68 of' the PacketCable must be set to a value of "1" (Network Signal).	Compliant
REQ5998	The Alerting Signal, Subject Audible Signal, Terminal Display Info, and Misc Signaling Information attributes must be present in the Signal Instance message generated in response to Condition 1 (Network Signal) if applied to the party under surveillance.	Compliant
REQ5999	When the generation of the Signal Instance message is due to Condition 2 in REQ5994, the Signal Type attribute in Table 68 of the PacketCable specification must be set to a value of "2" (Subject Signal).	Compliant
REQ6000	The Switch Hook Flash, Digits Dialed, and Misc Signaling Information attributes must be present in the Signal Instance message that is generated if the subject under surveillance receives any of these signaling instances.	Compliant

Table 2-4 Cisco BTS 10200 Release 5.0 Compliance with PKT-SP-EM 1.5-101-050128, Appendix A (continued)

Requirement	Description	Compliance
REQ6074 REQ6075 REQ6646 REQ6647 REQ6007 REQ6008 REQ6009 REQ6010 REQ6011 REQ6012	The required attributes must be present in the Signal Instance message as defined in the Comment section of Table 68 in the PacketCable specification.	Compliant
Section A.12, Conference Party Change		
REQ6648	The CMS must generate this event message for a conference call that was initiated by the user under surveillance when: • REQ6648.1—The subject adds a one or more additional parties to an existing call to form a conference call. • REQ6648.2—A party in a subject-initiated conference call is placed on hold. • REQ6648.3—A party in a subject-initiated conference call is retrieved from hold.	Compliant
REQ6649	The EM Header attribute must be present as the first attribute of the EM.	Compliant
REQ6650	Within the EM Header, the BCID must be one of the BCIDs associated with a call leg participating in the conference call.	Compliant
REQ6651	This attribute must be included when known, to identify all communicating parties, when the conference is established by the intercept subject's service.	Compliant
REQ6652	This attribute must be included when known, to identify a communicating party when one is added to the conference established by the intercept subject's service. This attribute can appear multiple times, one for each added party. This attribute can appear independently or in combination with other attributes.	Compliant
REQ6653	This attribute must be included when known, to identify a previously communicating party, when that party is removed (for example, placed on hold) from the conference established by the intercept subject's service. This attribute can appear multiple times, one for each removed party. This attribute can appear independently or in combination with other attributes.	Partially compliant (hold cases not addressed)
Section A.13, Surveillance Stop		
Not available	The CMS must timestamp this EM immediately at: 13—At the End of a call 14—When CMS determines that surveillance cannot be started, or can no longer be performed	Compliant

Table 2-4 Cisco BTS 10200 Release 5.0 Compliance with PKT-SP-EM 1.5-101-050128, Appendix A (continued)

Requirement	Description	Compliance
Not available	Surveillance Stop destination: • 1—Surveillance Stop applies to local surveillance only. • 2—Surveillance Stop applies to both local and remote surveillance. • 3 = Surveillance Stop applies only to remote surveillance.	Compliant
Not available	Surveillance Stop type: • 1—End of surveillance (CDC and, if present, CCC) • 2—End of CCC only (CDC to continue)	Compliant
Not available	Electronic Surveillance Indication This structure must be included when the local DF is not part of the DF chain (that is, the CMS has not established a DF chain by not including the ESI attribute in a Signaling Start EM). This structure must not be included when the local DF is part of the DF chain (that is, the CMS has established a DF chain by including the ESI attribute in a Signaling Start EM).	Compliant
Section A.14, Redirection		
Not available	The Redirection message must be sent to the DF if a call involving a surveillance subject is redirected and: • The CMS is aware of the redirection. • No Service Instance is generated for the redirection.	Compliant
Not available	The EM Header, Redirected From Party Number, Redirected To Party Number, Carrier Identification Code, and Related BCID attribute must be sent according to the requirements in Table 73 of the PacketCable Specification.	Compliant

Compliance with CALEA Requirements in PKT-SP-CMSS1.5-I01-050128 Section 7.7.2

Table 2-5 lists the requirements presented in the PacketCable specification PKTCBL 1.5 CMSS Section 7.7.2, Appendix D and indicates the level of compliance provided by the Enhanced CALEA feature for Cisco BTS 10200 Release 5.0.

Note The BTS 10200 does not originate a REFER message to the other CMS to transfer the call but can process the REFER message received from another CMS.

Table 2-5 Cisco BTS 10200 Release 5.0 Compliance with PKTCBL 1.5 CMSS Section 7.7.2, Appendix D

Requirement	Description	Compliance
Section 7.6.1, Procedures at Originating Exchange (REFER Method)		
REQ5025	The CMS originating a REFER must include additional header parameters for P-DCS-Billing-Info, and should include the additional header parameters for P-DCS-LAES, and P-DCS-Redirect, as specified in Section 7.7.	Not applicable BTS does not originate REFER message on CMSS trunk.

Table 2-5 Cisco BTS 10200 Release 5.0 Compliance with PKTCBL 1.5 CMSS Section 7.7.2, Appendix D **(continued)**

Requirement	Description	Compliance
Section 7.7.2, P-DCS-LAES		
REQ7454 REQ7455 REQ7456	The LAES-BCID field must always be present. The LAES-CCCID field must be present when the LAES-Content field is present. The LAES-Key field must not be included.	Compliant
REQ7457	When CMSO receives a 3XX Redirect response containing a P-DCS-LAES header in response to an INVITE, or receives a REFER request containing a P-DCS-LAES header in the Refer-To header for an active dialog, it must copy the received P-DCS-LAES header into the subsequent INVITE that is generated as a result of the REFER or Redirect.	Compliant
Section 7.7.2.2.1.1, Redirected Call Ends Early		
REQ7458	If CMSO receives a REFER request or 3XX Redirect response message as described above, but the call ends before the subsequent INVITE is sent (if, for example, the call is abandoned), then CMSO must send a Surveillance Stop message to its local DF containing the following information: • REQ7458.1—The local BCID already assigned to the call (this is a required field in the event message header) • REQ7458.2—The remote BCID assigned by CMST and received in the P-DCS-LAES header • REQ7458.3—The call-data IP address and port of the remote DF of CMST received in the P-DCS-LAES header • REQ7458.4—An indicator specifying that both call-data and call-content surveillance are to be stopped • REQ7458.5—An indicator specifying that the local surveillance session (if active) and remote surveillance session are to be stopped	Compliant
Section 7.7.2.2.1.2, P-DCS-LAES Header Cannot Be Included in Subsequent INVITE		
Section 7.7.2.2.1.2.1, CMSO Chooses to Perform Requested Surveillance		
REQ7459	If CMSO chooses to perform the requested call-data surveillance function, it must send a Signaling-Start message to its local DF containing the following information: • REQ7459.1—The local BCID already assigned to the call (this is a required field in the event message header) • REQ7458.6—The remote BCID assigned by CMST and received in the P-DCS-LAES header • REQ7459.2—The call-data IP address and port of the remote DF of CMST received in the P-DCS-LAES header	Compliant
REQ7460	If CMSO is already monitoring the call (for example, due to an outstanding lawfully authorized surveillance order on the originating subscriber) when it receives a P-DCS-LAES header, it must send a second Signaling-Start message to its local DF, containing the appropriate parameters as specified in the preceding item (REQ7459).	Compliant

Table 2-5 Cisco BTS 10200 Release 5.0 Compliance with PKTCBL 1.5 CMSS Section 7.7.2, Appendix D **(continued)**

Requirement	Description	Compliance
REQ7461	If the P-DCS-LAES header received in the 3XX Redirect response or REFER request also indicates that call content surveillance is to be performed (in addition to call data surveillance), then CMSO must allocate a local CCCID for the call and request the CMTS of the originating line (or MG of the originating trunk if the originator is off-net) to provide a copy of the call content to the local DF.	Compliant
REQ7462	In addition to the call-data information specified in REQ7459, CMSO must include the following data in the Signaling-Start message to the local DF: • REQ7462.1—The local CCCID assigned to the call. • REQ7462.2—The remote CCCID assigned by CMST and received in the P-DCS-LAES header. • REQ7462.3—The call-content IP address and port of the remote DF of CMST received in the P-DCS-LAES header. • REQ7462.4—When the call ends, CMSO must send a Surveillance-Stop message to its local DF containing the local BCID and indicating that both local and remote call-data and call-content surveillance are to be stopped.	Compliant
Section 7.7.2.2.1.2.2, CMSO Chooses to Perform Call-Data but Not Call-Content		
REQ7463	If the P-DCS-LAES header received in the 3XX Redirect response or REFER request indicates that both call-data and call-content surveillance are to be performed, but CMSO chooses to support only call-data (and not call-content), CMSO must send a Signaling-Start message to its local DF containing the call-data information specified in Section 7.7.2.2.1.2.1.	Compliant
REQ7464	CMSO must send a Surveillance-Stop message containing the following information: • REQ7464.1—The local BCID assigned by CMSO to the call. (This BCID was bound to the remote surveillance session by the previous Signaling-Start message.) • REQ7464.2—An indicator specifying that only the remote surveillance session is to be stopped. (This allows a local surveillance session that may be in progress on the originating endpoint to continue.) • REQ7464.3—An indicator specifying that (only) call-content surveillance is to be stopped. (This allows the remote call-data surveillance to continue.)	Compliant

Table 2-5 Cisco BTS 10200 Release 5.0 Compliance with PKTCBL 1.5 CMSS Section 7.7.2, Appendix D **(continued)**

Requirement	Description	Compliance
7.7.2.2.1.2.3 CMSO Chooses Not to Perform the Requested Surveillance		
REQ7465	If CMSO chooses not to perform any of the requested surveillance functions, it must send a Surveillance-Stop message to its local DF containing the following information: • REQ7465.1—The local BCID assigned by CMSO to the call. (Even though the local BCID is a required parameter, it does not convey any useful information in this case, because the local BCID was not bound to the remote surveillance session by a previous Signaling-Start message.) • REQ7465.2—The remote BCID assigned by CMST and received in the P-DCS-LAES header. • REQ7465.3—The call-data IP address and port of the remote DF of CMST received in the P-DCS-LAES header. • REQ7465.4—An indicator specifying that only the remote surveillance session is to be stopped. (This allows a local surveillance session that may be in progress on the originating endpoint to continue.)	Not applicable No scenario is identified where CMSO (if BTS) chooses not to perform the requested surveillance.
REQ7466	An indicator specifying that both call-data and call-content surveillance are to be stopped.	Not applicable No scenario is identified where CMSO (if BTS) chooses not to perform the requested surveillance.
Section 7.7.2.3.1, Terminating Line is Able to Accept the Call:		
REQ7467	If the terminating line is able to accept the call and a local outstanding lawfully authorized electronic surveillance order exists for the line or if a P-DCS-LAES header was received in the INVITE, CMST must send a Signaling-Start message to the local DF containing the identity of the terminating line and the local BCID assigned to the call. (The local BCID is a mandatory field.)	Compliant (Identity of terminating line is assumed to be defined as the phone number associated with the terminating line. Signaling start is sent for the terminating party as identified by the information in the INVITE message.) If the call is forwarded by the initial terminating party to another subscriber, the identify of the final terminating party should be derived from the last Redirection message associated with the call.

Table 2-5 Cisco BTS 10200 Release 5.0 Compliance with PKTCBL 1.5 CMSS Section 7.7.2, Appendix D **(continued)**

Requirement	Description	Compliance
REQ7468	If a P-DCS-LAES header was received, CMST must include the following additional information in the Signaling-Start message: • REQ7468.1—The remote BCID assigned by the remote CMS and received in the P-DCS-LAES header • REQ7468.2—The call-data IP address and port of the remote DF received in the P-DCS-LAES header	Compliant
REQ7469	If either the local electronic surveillance order or the received P-DCS-LAES header indicates that call-content surveillance is to be performed, the CMST must allocate a local CCCID for the call and request the CMTS of the terminating line (or MG of the terminating trunk if the terminator is off-net) in order to provide a copy of the call content to the local DF.	Compliant
REQ7470	In addition to the call-data parameters, the CMST must include the local CCCID in the Signaling-Start message it sends to the local DF.	Compliant
REQ7471	If a P-DCS-LAES header was received that indicates that call-content surveillance is to be performed, CMST must include the following additional information in the Signaling-Start message: • REQ7471.1—The remote CCCID assigned by the remote CMS and received in the P-DCS-LAES header • REQ7471.2—The call-content IP address and port of the remote DF received in the P-DCS-LAES header	Compliant
REQ7472	When the call ends, CMST must send a Surveillance-Stop message to its local DF containing the local BCID and indicating that both local and remote call-data and call-content surveillance are to be stopped.	Compliant
Section 7.7.2.3.2, Terminating Line Is Unable to Accept the Call		
REQ7473	If CMST receives an INVITE request containing a P-DCS-LAES header, and the terminating endpoint is not able to accept the call for some reason (for example, line is busy, line is unknown), and CMST does not need to otherwise initiate a surveillance session, CMST must send a Surveillance-Stop message containing the following information: • REQ7473.1—The local BCID assigned by CMST to this call **Note** To avoid affecting other surveillance sessions, CMST must use the BCID for this call and not the BCID of any other in-progress call on the same line. • REQ7473.2—The remote BCID received in the P-DCS-LAES header • REQ7473.3—The call-data IP address and port of the remote DF received in the P-DCS-LAES header • REQ7473.4—An indicator specifying that both call-data and (if active) call-content surveillance are to be stopped	Compliant

Table 2-5 Cisco BTS 10200 Release 5.0 Compliance with PKTCBL 1.5 CMSS Section 7.7.2, Appendix D **(continued)**

Requirement	Description	Compliance
Section 7.7.2.3.3, Terminating CMS Is Unable to Perform Call-Content Surveillance		
REQ7474	If CMST receives an INVITE containing a P-DCS-LAES header requesting call-data and call-content surveillance, and CMST is unable to perform the call-content surveillance for some reason (for example, call routed to voice mail server), CMST must continue to perform the call-data surveillance as specified in Section 7.7.2.3.1.	Compliant
REQ7475	Once this procedure has established the local-to-remote call-data surveillance information in the local DF, CMST must send a Surveillance-Stop message containing the following information: • REQ4857.1—The local BCID assigned to the terminating call • REQ4857.2—An indication that call-content surveillance is to be terminated	Compliant
Section 7.7.2.3.4, Terminating CMS Redirects or Transfers the Call		
REQ7476	If CMST is required to perform surveillance on a call (either as a result of terminating to a subscriber with a lawfully authorized surveillance order, or as specified in the P-DCS-LAES header of the INVITE message from the CMSO), but the call is redirected or transferred to a new terminating line, CMST must send a Signaling-Start message to the local DF containing the identity of the terminating line and the local BCID assigned to the call.	Compliant
REQ7477	If a P-DCS-LAES header was received, CMST must include the following additional information in the Signaling-Start message: • REQ7477.1—The remote BCID assigned by the remote CMS and received in the P-DCS-LAES header • REQ7477.2—The call-data IP address and port of the remote DF received in the P-DCS-LAES header	Compliant
REQ7478	If either the local electronic surveillance order or the received P-DCS-LAES header indicates that call-content surveillance is to be performed, CMST must allocate a local CCCID for the call.	Compliant
REQ7479	In addition to the call-data parameters, CMST must include the local CCCID in the Signaling Start message to the local DF.	Compliant
REQ7480	If a P-DCS-LAES header was received indicating that call-content surveillance is to be performed, then CMST must include the following additional information in the Signaling-Start message: • REQ7480.1—The remote CCCID assigned by the remote CMS and received in the P-DCS-LAES header • REQ7480.2—The call-content IP address and port of the remote DF received in the P-DCS-LAES header	Compliant
Section 7.7.2.3.4.1, CMST Sends REFER Request or Redirect Response[1]		
REQ7481	If CMST transfers or forwards the call by sending a REFER request or Redirect response to the originating CMS, then it must include a P-DCS-LAES header in the Redirect response or in the Refer-To header of the REFER request.	Compliant

Table 2-5 Cisco BTS 10200 Release 5.0 Compliance with PKTCBL 1.5 CMSS Section 7.7.2, Appendix D **(continued)**

Requirement	Description	Compliance
REQ7482	The P-DCS-LAES header must contain the following information: • REQ7482.1—The local BCID assigned to the call • REQ7482.2—The call-data IP address and port of the local DF	Compliant
REQ7483	If CMST is required to perform call-content surveillance for the call, it must include the following additional data in the P-DCS-LAES header: • REQ7483.1—The local CCCID assigned to the call • REQ7483.2—The call-content IP address and port of the local DF	Compliant
REQ5178	If the P-DCS-LAES header is present in the 183-Session-Progress response (indicating surveillance is required on the terminating subscriber, but that the terminating equipment is unable to perform that function), CMSO must include this information in the Authorization for Quality of Service, or must signal this information to the device performing the intercept (for example, a media gateway).	Compliant
REQ5221 REQ5349	If a P-DCS-LAES header is present in the 3xx response, CMSO should include that header unchanged in the reissued INVITE.	Compliant

1. The BTS 10200 does not support sending a REFER message.

CHAPTER 3

Subscriber Features

Revised: March 24, 2011, OL-12606-21

The Cisco BTS 10200 Softswitch supports subscriber features, including selected custom local area signaling service (CLASS) features, as described in the following sections. Most of these features are defined in Telcordia LSSGR documents or in corresponding ITU-T documents. In most cases, The BTS 10200 features delivered via gateway clients behave identically to their PSTN counterparts. These features are described in the following sections:

- Call Forwarding Features
- Call Waiting Features
- Calling Identity Features
- Direct Inward/Outward Dialing for PBX
- Features for Centrex Subscribers Only
- Additional Features Applicable to Centrex and POTS

Additional general information is provided in the following sections:

- Office Service ID and Default Office Service ID
- Notes on Bundling Features in Services

Note For network features, see Chapter 1, "Network Features." For outgoing call restriction options (Class of Service and Outgoing Call Barring), see Chapter 4, "Class of Service Restrictions and Outgoing Call Barring Features."

Some features can be accessed and controlled by the subscriber using a handset and vertical service codes (VSCs). VSCs are provisionable by the service provider (any valid unique ASCII string up to five characters long), and the customary values are country specific. The VSC values used throughout this chapter are for illustration purposes. For convenience, some VSC values are preprovisioned in the BTS 10200. The valid formats for VSC ASCII strings are listed in the Vertical Service Code commands in the *Cisco BTS 10200 Softswitch CLI Database*. To view the current VSC values provisioned on your system, use the **show vsc** CLI command. To provision VSCs, see the VSC provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Typically, the system responds to user handset actions by providing an appropriate announcement. However, if an announcement is not provisioned or cannot be played, an appropriate tone (confirmation tone or reorder tone) is played. A list of these announcements and tones is provided in Appendix A - Cause Code to Announcement ID Mappings" in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Tip For information on provisioning these features, see the Feature Provisioning chapter in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Interoperability

The BTS 10200 interworks with a wide range of network elements (NEs), but there are certain limitations. Cisco recommends that you keep the following caution in mind as you prepare to purchase and use NEs for your network.

Caution Some features involve the use of other network elements (NEs) deployed in the service provider network, for example, gateways, media servers, announcement servers, eMTAs, and SIP phones. See the "Component Interoperability" section of the *Release Notes* for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the Cisco BTS 10200 Softswitch Release 5.0 software. Earlier or later releases of platform software might be interoperable and it might be possible to use other functions on these platforms. The list in the *Release Notes* certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the Cisco BTS 10200 Softswitch.

Subscriber Feature List

Table 3-1 lists the subscriber features that are described in this chapter, an industry reference document (if applicable), and the category of subscriber for which this service is available.

Table 3-1 Subscriber Features

Feature Description	Industry Reference Document	Subscriber Category
Call Forwarding Features		
Call Forwarding Unconditional (CFU)	FSD 01-02-1401 GR-580	Centrex POTS
Call Forwarding Variable for Basic Business Group (CFVBBG)	FSD 01-02-1450 GR-586	Centrex POTS
Remote Activation of Call Forwarding (RACF)		Centrex POTS
Remote Call Forwarding (RCF)	FSD 01-02-1450 GR-586	Centrex POTS
Call Forwarding Busy (CFB)	FSD 01-02-1450 TR-TSY-000586	Centrex POTS

Table 3-1 Subscriber Features (continued)

Feature Description	Industry Reference Document	Subscriber Category
Call Forwarding No Answer (CFNA)	FSD 01-02-1450 TR-TSY-000586 FSD 01-02-2200 TR-TSY-001520	Centrex POTS
Call Forwarding Combination (CFC)		Centrex POTS
Call Waiting Features		
Call Waiting (CW)	FSD 01-02-1201 TR-NWT-000571	Centrex POTS
Cancel Call Waiting (CCW)	FSD 01-02-1204 TR-TSY-000572	Centrex POTS
Calling Identity Delivery on Call Waiting (CIDCW)	FSD 01-02-1090 TR-NWT-000575	Centrex POTS
Call Waiting Deluxe (CWD)		Centrex POTS
Calling Identity Features		
Calling Identity Delivery • Calling Number Delivery (CND) • Calling Name Delivery (CNAM)	FSD 01-02-1051 GR-31-CORE FSD 01-02-1070 TR-NWT-001188	Centrex POTS
Calling Line Identification Presentation (CLIP)	FSD 01-02-1051 GR-31-CORE and ITU-T Recommendation I.251.3 (08/92)	Centrex POTS
Calling Identity Delivery Blocking (CIDB) • Calling Number Delivery Blocking (CNDB) • Calling Name Delivery Blocking (CNAB) • Calling Identity Delivery and Suppression (CIDSD and CIDSS)	FSD 01-02-1053 GR-391-CORE	Centrex POTS

Table 3-1 Subscriber Features (continued)

Feature Description	Industry Reference Document	Subscriber Category
Calling Line Identification Restriction (CLIR) • Calling Number Delivery Blocking (CNDB) • Calling Name Delivery Blocking (CNAB) • Calling Identity Delivery and Suppression (CIDSD and CIDSS)	FSD 01-02-1053 GR-391-CORE and ITU-T Recommendation I.251.4 (08/92)	Centrex POTS
Seasonal Suspend (Not available for Centrex and MLHG subscribers)		
Terminal and Group Make Busy Services		
Direct Inward/Outward Dialing for PBX		
• Analog DID for PBX	TIA/EIA-464B	POTS only
• DOD For PBX	FSD 04-02-0000 TR-TSY-000524	POTS only
Features for Centrex Subscribers Only		
Call Hold (CHD)	FSD 01-02-1305 TR-TSY-000579	Centrex only
Call Park and Call Retrieve	FSD 01-02-2400 GR-2913-CORE	Centrex only
Direct Inward/Outward Dialing for Centrex	FSD 01-01-1000 TR-TSY-000520	Centrex only
Directed Call Pickup (With and Without Barge-In)	FSD 01-02-2800 TR-TSY-000590	Centrex only
Distinctive Alerting/Call Waiting Indication (DA/CWI)	FSD 01-01-1110 GR-520-CORE	Centrex only
Additional Features Applicable to Centrex and POTS		
Anonymous Call Rejection (ACR)	FSD 01-02-1060 TR-TSY-000567	Centrex POTS
Automatic Callback (AC)—Repeat Dialing	GR-215-CORE	Centrex POTS
Automatic Recall (AR)—Call Return	GR-227-CORE	Centrex POTS
Call Block - Reject Caller (CBLK)		Centrex POTS
Call Transfer (CT)	FSD 01-02-1305 TR-TSY-000579	Centrex POTS

Table 3-1 Subscriber Features (continued)

Feature Description	Industry Reference Document	Subscriber Category
Customer-Originated Trace (COT)	FSD 01-02-1052 GR-216-CORE	Centrex POTS
Do Not Disturb (DND)	FSD 01-02-750 SR-504	Centrex POTS
Hotline Service (See also "Hotline-Variable Service (HOTV)" and "Warmline Service")		Centrex POTS
Hotline-Variable Service (HOTV)		Centrex POTS
Interactive Voice Response (IVR) Functions		Centrex POTS
Limited Call Duration Service (Prepaid/Postpaid) with RADIUS Interface to AAA		POTS
Message Waiting Indicator (MWI)—Audible and Visual		Centrex POTS
Multiline Hunt Group (MLHG)	FSD 01-02-0802 TR-TSY-000569	Centrex POTS
Multiline Variety Package		Centrex POTS
Multiple Directory Numbers (MDN)		POTS only
No Solicitation Announcement (NSA)		Centrex POTS
Privacy Screening (Calling Identity with Enhanced Screening)		Centrex POTS
Speed Call • Speed Call for Individual Subscribers • Group Speed Call (Centrex and MLHG only)	FSD 01-02-1101 TR-TSY-000570	Centrex POTS

Table 3-1 Subscriber Features (continued)

Feature Description	Industry Reference Document	Subscriber Category
Subscriber-Controlled Services and Screening List Editing (SLE) • Selective Call Forwarding (SCF) • Selective Call Acceptance (SCA) • Selective Call Rejection (SCR) • Distinctive Ringing/Call Waiting (DRCW)	FSD 30-28-1000 GR-220-CORE FSD 01-02-1410 TR-TSY-000217 FSD 01-02-0760 TR-TSY-000218 FSD 01-01-1110 TR-TSY-000219	Centrex POTS
Temporarily Disconnected Subscriber Status and Soft Dial Tone		Centrex POTS
Three-Way Calling (TWC)	FSD 01-02-1301 TR-TSY-000577	Centrex POTS
Three-Way Calling Deluxe (TWCD)		Centrex POTS
Usage-Sensitive Three-Way Calling (USTWC)	FSD 01-02-1304 TR-TSY-000578	Centrex POTS
Visual Message Waiting Indicator (VMWI)	GR-2942-CORE	Centrex POTS
Voice Mail (VM) and Voice Mail Always (VMA)		Centrex POTS
Warmline Service (See also "Hotline Service")		Centrex POTS

Call Forwarding Features

Call forwarding is a group of features allowing incoming calls to a subscriber line to be forwarded to another telephone number, including a cellular phone number, under various circumstances. Call forwarding features allow a subscriber line to be forwarded to a number that itself can be forwarded. This chaining of call forwards is allowed to a maximum of five different stations as long as none of the station numbers appears twice in the forwarding list (in order to prevent loops). Before forwarding a call outside of a zone or off net, the system must determine if the forwarding station already has an active call that has been forwarded to the same destination. If so, forwarding is denied to the second call and a station busy signal is returned to the caller.

The following types of call forwarding features are provided by the Cisco BTS 10200 Softswitch:

- Call Forwarding Unconditional (CFU)
- Call Forwarding Variable for Basic Business Group (CFVBBG)

- Remote Activation of Call Forwarding (RACF)
- Remote Call Forwarding (RCF).
- Call Forwarding Busy (CFB)
- Call Forwarding No Answer (CFNA)
- Call Forwarding Combination (CFC)
- Call Forwarding Redirection (CFR)—This is a SIP-specific feature. With CFR, the SIP endpoint initiates the call forwarding. For a description and provisioning commands, see the "Sending 302 on Call Redirection" section in the *Cisco BTS 10200 Softswitch SIP Feature and Provisioning Guide*.

Call Forwarding Unconditional (CFU)

The Cisco BTS 10200 Softswitch provides the call forwarding unconditional (CFU) feature. CFU allows the user to forward all calls regardless of the status of the user's line. A typical forwarding address is voice mail, a remote telephone, or an attendant.

Reference documents include:

- LSSGR module FSD 01-02-1401 (GR-580), *Call Forwarding Variable*
- LSSGR module FSD 01-02-1450 (GR-586), *Call Forwarding Subfeatures*
- ITU-T Q-732.2
- ITU I-252.4

The service provider can provision the CFU feature to be active immediately on the customer line, or to be activated by the individual subscriber using the handset. The user activates the CFU feature on the local phone, and enters the forward-to phone number where the user wishes to have the calls forwarded. This forward-to directory number (DN) is referred to as the B-number. The allowed types of B-numbers are listed in Table 3-2.

Table 3-2 Allowed Types of B-numbers

Subscriber Type	Allowed B-number
POTS	DN, without extensions
Centrex	Public access code + external DN, without extensions
	An extension within the business group

The following conditions apply to the CFU feature:

- The CFU feature can be provided to POTS, Centrex, and MLHG subscribers.
- The CFU feature is in the deactivated mode unless activated by the service provider or subscriber.
- Call forwarding hop scenarios are restricted to a maximum of five hops. The call will be completed on the provisioned maximum number of hops.

The CFU feature is composed of four associated features, which are described in the following sections:

- CFU Activation (CFUA), page 3-8
- CFU Deactivation (CFUD), page 3-10
- CFU Interrogation (CFUI), page 3-11
- CFU Invocation, page 3-11

Additional information about this feature is covered in the following sections:

- Invalid User Actions, page 3-11
- CFU Feature Interactions, page 3-12
- Feature Provisioning Commands, page 3-13

CFU Activation (CFUA)

This section discusses how the service provider can customize CFU activation, and the CFU activation procedures available to the handset user.

Blocking Call Forwarding to Certain Types of DNs

The service provider can block call forwarding to certain types of DNs by provisioning the nature of dial (NOD) parameter for the call-forwarding features (CFU, CFB, CFNA, and CFC) in the NOD Restrict List (nod-restrict-list) table. For example, if you provision NOD=TOLL-FREE and NOD=EMG in the nod-restrict-list table, the system will not allow call-forwarding to DNs of those types.

Caution If you want to block call-forwarding to an emergency (EMG) DN, such as 911, you must provision NOD=EMG for the call-forwarding features (CFU, CFB, CFNA, and CFC) in the NOD-RESTRICT-LIST. This is necessary to comply with the rule in Telcordia document GR-580, which says that 911 should not be a permitted “forward to” number.

Tip To provision the CFU feature, see the CFU provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

CFUA Customization Options

The behavior of CFU activation can be customized using the following provisionable options.

- Courtesy call (CC)—The CC flag controls the delivery of a courtesy call while activating CFU.
  - A value of N indicates that no courtesy call will be placed.
  - A value of ANS or NOANS indicates that a courtesy call will be placed. ANS means that the courtesy call will have to be answered for CFU to be activated. NOANS means that the courtesy call does not have to be answered for CFU to be activated.
- Second stage dial tone (SDT)—The SDT flag controls the delivery of a dial tone after the subscriber enters the vertical service code (VSC) for activation or interrogation of CFU. The permitted values for this flag are:
  - NO_TONE
  - DIAL_TONE
  - STUTTER_DIAL_TONE
  - CONFIRMATION_TONE
  - CONFIRMATION_DIAL_TONE

Note For SIP phone subscribers, the SDT parameter has no effect. The SDT option is available through the dial plan in the SIP phone.

- Final stage dial tone (FDT)—The FDT flag controls the system response to a successful activation, deactivation, or interrogation of CFU by the subscriber. If FDT is not provisioned, the system provides a success announcement. The permitted values for this flag are the same as for the SDT flag.

Note For SIP phone subscribers, only the success announcements will be provided. The confirmation tone and dial tone will not be provided, even if the FDT flag is set.

- Reminder ring (RR)—When RR is provisioned as Y, a subscriber who has an idle station with CFU activated, receives a reminder ring when incoming calls are forwarded. If the subscriber goes off-hook after hearing the RR, the system ignores the off-hook condition, and does not complete the call to this station; the call is forwarded to the DN provisioned for CFU. A reminder ring is a half-second burst of ringing. The reminder ring is not applied when the forwarding station is off hook.
- Multiple call forwarding (MCF)—When MCF is provisioned as Y, the system allows multiple incoming calls to be forwarded by the subscriber at the same time. If a subscriber already has CFU invoked, additional calls to the subscriber will be forwarded by CFU based on the MCF flag. If the MCF flag is set to N, the system allows only one CFU invocation.
- International call forwarding (INTL)—When the INTL flag is set to N, the system does not allow forwarding to an international number. When INTL is set to Y, the system checks for other restrictions on international calls, and allows forwarding if there are no other restrictions provisioned for the call type and calling number. (Other provisionable restrictions on international calling can be based on the nature of dial [NOD] and the subscriber feature data.)

To view a list of these feature options for CFU in the *Cisco BTS 10200 Softswitch CLI Database*, use the **show feature-profile-base fname=cfu** CLI command.To provision the CFU feature, see the CFU provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

CFUA Handset Procedures

CFU can be activated by the service provider or by the individual user. The procedures are as follows:

- CFU can be activated permanently at subscription time by the service provider. The service provider provisions the forward-to DN as requested by the subscriber. All calls made to the subscriber's line will be forwarded to the single forward-to number that was provisioned.
- CFU can be activated by the user as follows.

Note See the "CFUA Customization Options" section on page 3-8 for details of customized features CC, SDT, and FDT.

  - The user lifts the handset and listens for dial tone.
  - The user presses the VSC applicable to CFU activation (for example, typically *72 in North America and *57* in China). The VSC values are provisionable by the service provider.
  - If provisioned for SDT, and if CFU can be activated, the system returns the provisioned dial tone.

- The user enters the B-number (local, long distance, or international) where calls are to be forwarded.
- The user receives an appropriate error announcement if the forward-to number is invalid or restricted, or if the feature cannot be activated.
- If the feature can be activated to the forward-to number entered, the system returns a confirmation tone and attempts to place a courtesy call to the forward-to number (if provisioned for CC).
- If the forwarded-to party answers the courtesy call (when CC is provisioned as ANS), or if CC is provisioned as NOANS, the CFU feature is activated.

Note When CC is provisioned for ANS, and if the forwarded-to line is busy or does not answer, the CFU feature is not activated. The user can still activate CFU by repeating the activation procedure within 2 minutes of the first attempt. No courtesy call is set up during the second attempt. The user hears a confirmation tone. If more than 2 minutes elapse before the second attempt, the second attempt is treated as a first attempt.

- If FDT is provisioned, the user hears a confirmation tone for 1 second, followed by the provisioned dial tone, indicating that activation was successful. If FDT is not provisioned, the user hears a success announcement.

Note FDT and CC are mutually exclusive—The system never provides FDT if a courtesy call is placed during the activation attempt (whether or not the courtesy call is answered). FDT is only provided, if provisioned, when a courtesy call is not involved.

- CFU is now activated, and will stay active until it is deactivated with the appropriate deactivation VSC, or is overridden by the service provider via a CLI command.

CFU Deactivation (CFUD)

CFU can be deactivated by the service provider via a CLI command. Alternatively, CFU can be deactivated by the individual user as follows:

Note See the "CFUA Customization Options" section on page 3-8 for details of the customized feature FDT.

- The user lifts the handset and listens for dial tone.
- The user presses the VSC applicable to CFU deactivation (for example, typically *73 in North America and #57# in China). The VSC values are provisionable by the service provider.
- The user receives an appropriate error announcement if the feature cannot be deactivated.
- If deactivation was successful, and if FDT is provisioned, the user hears a confirmation tone for 1 second, followed by the provisioned dial tone. If FDT is not provisioned, the user hears a success announcement.
- CFU is now deactivated, and will stay deactivated until it is activated with the appropriate activation VSC, or is overridden by the service provider via a CLI command.

CFU Interrogation (CFUI)

CFU interrogation allows a user to check whether CFU is activated to a particular phone. The user performs an interrogation as follows.

Note See the "CFUA Customization Options" section on page 3-8 for details of customized features SDT and FDT.

- The user lifts the handset and listens for dial tone.
- The user presses the VSC applicable to CFU interrogation (for example, typically *#57* in China). The VSC values are provisionable by the service provider.
- If provisioned for SDT, and if CFU can be interrogated, the system returns the provisioned dial tone. If not provisioned for SDT, no tones are provided.
- The user enters the forward-to number to be interrogated (B-number).

Note The user can follow the B-number with a # to indicate the end of B-number entry.

Note If the user enters a digit string that does not match exactly the B-number against which CFU was activated, the interrogation attempt results in an error announcement.

- The user receives an appropriate error announcement if the CFU feature is not forwarded to the B-number entered, or if the B-number is invalid.
- If FDT is provisioned and the CFU feature is activated to the forward-to number entered, the user hears a confirmation tone for 1 second, followed by the provisioned dial tone.
- If FDT is not provisioned and the CFU feature is activated to the forward-to number entered, the system returns a success announcement.

CFU Invocation

CFU invocation is the actual procedure the system follows to forward the call.

Invalid User Actions

The following user actions are invalid, and the system provides an appropriate error announcement:

- The user enters an invalid directory number (DN) for the B-number.
- The user tries to activate CFU (with CC set to ANS) for the second time within a 2-minute interval to a DN which is different from the one used in the first attempt. (In addition, the history associated with the first attempt will be removed.)
- During CFU activation, the user enters a B-number that is determined by the system to be a type blocked by provisioning in the NOD-RESTRICT-LIST table. For example, if the nature of dial (NOD) for the B-number is set to EMG (emergency), but calls with NOD=EMG are blocked by provisioning in the NOD-RESTRICT-LIST table, the activation to that B-number will be denied.

- The user tries to activate CFU from a DN that has outgoing calls blocked by the OCB feature, or the user enters a B-number, but calls to that DN are blocked by OCB. For example, the call from the user's phone to the B-number would be a domestic long-distance call, but these calls are blocked by setting K=2 against the OCB feature in the SUBSCRIBER-FEATURE-DATA table.

Note The database tables (NOD-RESTRICT-LIST and SUBSCRIBER-FEATURE-DATA) mentioned in the above list are described in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*. For information on billing records, see the *Cisco BTS 10200 Softswitch Billing Reference Guide*. For information on measurements, see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

- The user tries to activate CFU from or to a DN for which calls are restricted by the COS feature.
- The user tries to activate CFU when already activated (the B-number is not overwritten).
- The user tries to activate CFU to an international DN, but the service provider has blocked forwarding to international DNs. The service provider can block forwarding to international DNs using the international flag in the FEATURE table.
- The user tries to activate CFU to his or her own extension or DN.
- The user tries to deactivate CFU when already deactivated.
- The user interrogates CFU, but enters a digit string that does not match exactly the B-number against which CFU was activated. For example, if CFU was activated with a 5-digit string corresponding to a Centrex extension, and interrogation is attempted using a 10-digit string of the complete DN, the interrogation attempt will result in an error announcement. (See the complete list of standard Cisco BTS 10200 announcements in the *Cisco BTS 10200 Softswitch Provisioning Guide*.)
- The user tries to interrogate CFU on a fresh system (a system with no entry in the SUBSCRIBER-FEATURE-DATA table). In this case, the user receives the error announcement immediately after entering the interrogation code (for example, *#57*). The system does not wait for the user to enter the B-number

CFU Feature Interactions

This section describes the interaction of other subscriber features with the CFU feature.

- CLIP, CNAM, and CND (caller ID features)—When a call is forwarded, the forwarded-to party receives the DN of the calling party on the caller ID display.
- OCB—The interaction of CFU and OCB depends upon the sequence in which they are activated:
  - If OCB is activated prior to CFU activation—OCB screening is performed on each DN the user enters when attempting to activate CFU. Successful CFU activation depends on the existing OCB K-VALUE and the forward-to DN:

Note If the existing OCB K-VALUE is set to block calls to the forward-to DN, then the system does not allow CFU activation. The user receives an error announcement.

Note If the OCB K-VALUE allows calls to this DN, then the CFU activation process continues. Once the CFU activation attempt to a specific DN is accepted by the system, it is applicable permanently regardless of any future OCB K-VALUE changes. That is, future changes to the OCB K-VALUE have no effect on CFU invocation. CFU to this DN can be deactivated by the user in the normal manner (#57#).

- If CFU is activated prior to OCB activation—The user can activate the OCB feature, or change the OCB K-VALUE, regardless of the existing CFU feature. However, invocation of OCB depends upon the type of call:

Note User-dialed calls—User-dialed calls can be blocked by OCB (depending on the K-VALUE).

Note Forwarded calls—CFU remains active as originally set up by the user, therefore, calls forwarded by the CFU feature ***cannot*** be blocked using OCB screening.

- COS—If a call to a DN is restricted by COS screening, CFU cannot be activated or invoked to that DN.
- If a subscriber has CFU activated and the operator attempts to use the BLV or OI functions, the operator will receive a busy tone and will not be able to perform an interrupt on the call.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the CFU provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Call Forwarding Variable for Basic Business Group (CFVBBG)

This section describes the CFVBBG feature and its associated features—CFVABBG, CFUD, and CFUI.

CFVBBG Description

Call Forwarding Variable for Basic Business Group (CFVBBG) is the CFU variant for BBG subscribers with Centrex service. It has the same behavior as CFU, except that it uses CFVABBG as its associated activation feature. Associating CFVABBG causes different treatment of the courtesy call while activating CFVBBG.

Note The other associated features for CFVBBG are CFUD and CFUI. These associated features behave the same as described in the "CFU Deactivation (CFUD)" and "CFU Interrogation (CFUI)" sections.

Note CFUA is *not* an allowed associated feature for CFVBBG.

The following limitations and behaviors apply to CFVBBG:

- CFVBBG can be provided to Centrex and MLHG subscribers only.
- All feature interactions for CFVBBG are the same as for CFU.
- CFVBBG logs the billing record as a CFU record.
- CFVBBG generates measurements as CFU measurements.

CFVBBG Activation—CFVABBG

The system provides a BBG feature variant of CFUA called CFVABBG. For BBG subscribers, it is not recommended to deliver a courtesy call to a forwarded-to extension of another internal BBG line while activating forwarding. Other mechanics of operation of this feature are the same for CFVABBG as for CFUA, except that the courtesy call (CC) flag is always turned off.

The following limitations and behaviors apply to CFVABBG.

Note See the "CFUA Customization Options" section on page 3-8 for details of the CC flag.

- CFVABBG can only be assigned to Centrex (BBG) subscribers.
- For typical business group call forwarding treatment, it is recommended to set the CC flag to N. In this case, CFVABBG implements the following courtesy call treatment during activation:
  - When activated to an extension, no courtesy call is placed.
  - When activated to an outside line, a courtesy call is placed. If the forwarded-to party answers the courtesy call, the feature is activated.

  Note If the forwarded-to line is busy or does not answer, the feature is not activated. The user can still activate CFVBBG by repeating the activation procedure within 2 minutes of the first attempt. No courtesy call is set up during the second attempt. The user hears a confirmation tone. If more than 2 minutes elapse before the second attempt, the second attempt is treated as a first attempt.
- CFVABBG uses the NOD-RESTRICT-LIST entry for CFU.
- Activating CFVBBG will create a record in the SUBSCRIBER-FEATURE-DATA table with FNAME as CFU.
- All feature interactions for CFVABBG are the same as for CFUA.
- CFVABBG logs the billing record as a CFUA record.
- CFVABBG generates measurements as CFUA measurements.

Note The database tables (NOD-RESTRICT-LIST and SUBSCRIBER-FEATURE-DATA) mentioned in the above list are described in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*. For information on billing records, see the *Cisco BTS 10200 Softswitch Billing Reference Guide*. For information on measurements, see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the CFVBBG provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Remote Activation of Call Forwarding (RACF)

Remote activation of call forwarding (RACF) permits user s to control their CFU functions when they are away from the phone. The service provider sets up this function for the user, and designates a DN the user should call to access interactive voice response (IVR) functions that control the RACF feature. Once the RACF function is set up, the user can take the following actions from a remote station:

- Activate CFU
- Deactivate CFU
- Change the target DN of CFU

The procedure is similar to making call-forwarding changes at a home or local business phone, but requires the additional step of dialing the remote location:

- The user dials a remote-access DN and is prompted to enter the directory number of the home or local business phone and then the RACF authorization code (a personal identification code, PIN). The PIN can be shared by a group, or can be unique to the individual subscriber.

  Note A shared (nonunique) PIN is usually assigned to the subscriber group by the service provider. It can be changed only by the service provider, and not through handset provisioning.

- Upon successful validation of the PIN, the user's current CFU activation status is checked.
  - If the CFU feature is currently inactive (calls are not being forwarded), the user is prompted to enter a DN to which calls should be forwarded.
  - If the CFU feature is currently active (calls are being forwarded), the user is given the option of deactivating CFU or changing the DN to which call should be forwarded.

Note When the user accesses the RACF function, and enters (or changes) the DN to which calls are forwarded, the system checks the validity of the forwarded number.

- A subscriber with a unique PIN can change the PIN using the VSC function. (A specific VSC, for example *98, is assigned and provisioned by the service provider.) The PIN can only be changed from the base phone.

Tip For more details about the IVR interactions for this feature, see Chapter 6, "Interactive Voice Response Functions."

Tip To provision this feature, see the RACF provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Remote Call Forwarding (RCF)

The Cisco BTS 10200 Softswitch implements the remote call forwarding (RCF) feature as specified in LSSGR module FSD 01-02-1450 (GR-586), *Call Forwarding Subfeatures*.

RCF allows all incoming calls to be routed automatically to a remote DN, which can be in another region (NANP area for North America). RCF is activated by the service provider at customer request. With the RCF feature, all calls to the specified DN are always forwarded to a remote address. This service is similar to the CFU service with these exceptions:

- Forwarding is always activated and not controlled by the customer. (The forwarded-to number cannot be changed by direct customer action.)
- No local office terminal (physical telephone) is associated with the dialed number from which forwarding occurs.
- Multiple simultaneous calls can be active between the base switching office and the remote RCF terminal.

The billing data produced by the Cisco BTS 10200 Softswitch identifies the invoked feature as CFU and not RCF. The calling party is charged for the call to the RCF DN. The called party (RCF DN) can be charged for the CFU feature usage. The service provider can also charge the called party (RCF DN) for the call from the RCF base DN to the remote DN.

Tip To provision this feature, see the RCF provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Call Forwarding Busy (CFB)

The Cisco BTS 10200 Softswitch provides the call forwarding busy (CFB) feature. CFB allows a user (the called party) to instruct the network to forward calls when the line is busy or unreachable. A typical forwarding number is voice mail. The forwarding station is off hook when the CFB feature is executed, therefore no reminder ring is generated. CFB is set up by the service provider at the subscriber's request.

Note A specific trigger, T_NOT_REACHABLE, must be provisioned for the CFB feature to enable the call forwarding on unreachable condition.

Reference documents include:

- LSSGR module FSD 01-02-1401 (GR-580), *Call Forwarding Variable*
- LSSGR Module FSD 01-02-1450 (GR-586), *Call Forwarding Subfeatures*
- ITU-T Q-732.2
- ITU I-252.4

The service provider can provision the CFB feature to be active immediately on the customer line, or to be activated by the individual subscriber using the handset. The user activates the CFB feature on the local phone, and enters the forward-to phone number where the user wishes to have the calls forwarded. This forward-to DN is referred to as the B-number. The allowed types of B-numbers are listed in Table 3-3.

Table 3-3 Allowed Types of B-numbers

Subscriber Type	Allowed B-number
POTS	DN, without extensions
Centrex	Public access code + external DN, without extensions
	An extension within the business group

The following conditions apply to the CFB feature:

- The CFB feature can be provided to POTS, Centrex, and MLHG subscribers.
- The CFB feature is in the deactivated mode unless activated by the service provider or subscriber.
- Call forwarding hop scenarios are restricted to a maximum of five hops. The call will be completed on the provisioned maximum number of hops.
- Multiple call forwarding (MCF) is a provisionable option that allows multiple incoming calls to be forwarded by the subscriber at the same time. If a subscriber already has CFB invoked, additional calls to the subscriber will be forwarded by CFB based on the MCF flag. If the MCF flag is turned off, only one CFB invocation is allowed.

The CFB feature is composed of four associated features, which are described in the sections that follow:

- CFB Variable Activation (CFBVA), page 3-17
- CFB Variable Deactivation (CFBVD), page 3-20
- CFB Interrogation (CFBI), page 3-20
- CFB Invocation, page 3-21

Additional information about this feature is covered in the following sections:

- Invalid User Actions, page 3-21
- CFB Feature Interactions, page 3-22
- Feature Provisioning Commands, page 3-23

CFB Variable Activation (CFBVA)

This section discusses how the service provider can customize CFBVA, and the CFBVA procedures available to the handset user.

Blocking Call Forwarding to Certain Types of DNs

The service provider can block call forwarding to certain types of DNs by provisioning the nature of dial (NOD) parameter for the call-forwarding features (CFU, CFB, CFNA, and CFC) in the NOD Restrict List (nod-restrict-list) table. For example, if you provision NOD=TOLL-FREE and NOD=EMG in the nod-restrict-list table, the system will not allow call-forwarding to DNs of those types.

Caution If you want to block call-forwarding to an emergency (EMG) DN, such as 911, you must provision NOD=EMG for the call-forwarding features (CFU, CFB, CFNA, and CFC) in the NOD-RESTRICT-LIST. This is necessary to comply with the rule in Telcordia document GR-580, which says that 911 should not be a permitted "forward to" number.

Tip To provision the CFB feature, see the CFB provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

CFBVA Customization Options

The behavior of CFBVA can be customized using the following provisionable options. The detailed provisioning steps for these options are provided in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

- Courtesy call (CC)—The CC flag controls the delivery of a courtesy call while activating CFB. Although this option can be provisioned, as a practical matter it usually is not provided with CFB service in most markets.
- Second stage dial tone (SDT)—The SDT flag controls the delivery of a dial tone after the subscriber enters the VSC for activation or interrogation of CFB. The permitted values for this flag are:
  - NO_TONE
  - DIAL_TONE
  - STUTTER_DIAL_TONE
  - CONFIRMATION_TONE
  - CONFIRMATION_DIAL_TONE

  Note For SIP phone subscribers, the SDT parameter has no effect. The SDT option is available through the dial plan in the SIP phone.

- Final stage dial tone (FDT)—The FDT flag controls the system response to a successful activation, deactivation, or interrogation of CFB by the subscriber. If FDT is not provisioned, the system provides a success announcement. The permitted values for this flag are the same as for the SDT flag.

  Note For SIP phone subscribers, only the success announcements will be provided. The confirmation tone and dial tone will not be provided, even if the FDT flag is set.

- Multiple call forwarding (MCF)—When provisioned as Y, MCF allows multiple incoming calls to be forwarded by the subscriber at the same time. If a subscriber already has CFB invoked, additional calls to the subscriber will be forwarded by CFB based on the MCF flag. If the MCF flag is set to N, only one CFB invocation is allowed.

- International call forwarding (INTL)—When the INTL flag is set to N, forwarding to an international number is not allowed. When INTL is set to Y, the system checks for other restrictions on international calls, and allows forwarding if there are no other restrictions provisioned for the call type and calling number. (Other provisionable restrictions on international calling can be based on the nature of dial (NOD) and the subscriber feature data.)

Detailed information on how to set these parameters is provided in the following documents:

- The "Valid Features" appendix in the *Cisco BTS 10200 Softswitch Command Line Interface Guide for Call Processing* lists all of the TYPE/VALUE pairs that are valid for each feature, including FDT, SDT, CC, and so forth.
- The "Feature Profile Base" section in the "Valid Features" appendix of the *Cisco BTS 10200 Softswitch Command Line Interface Guide for Call Processing* provides descriptions of the TYPE/VALUE pairs.
- The CFU provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide* lists the provisioning commands to use with these parameters.

CFBVA Handset Procedures

CFB can be activated by the service provider or by the individual user. The procedures are as follows:

- CFB can be activated permanently at subscription time by the service provider. The service provider provisions the forward-to DN as requested by the subscriber. When the phone is off hook, calls made to the subscriber's line will be forwarded to the single forward-to number that was provisioned.
- CFB can be activated by the user as follows.

Note See the "CFBVA Customization Options" section on page 3-18 for details of customized features CC, SDT, and FDT.

  - The user lifts the handset and listens for dial tone.
  - The user presses the VSC applicable to CFB activation (for example, typically *90 in North America and *40* in China). The VSC values are provisionable by the service provider.
  - If provisioned for SDT, and if CFB can be activated, the system returns the provisioned dial tone.
  - The user enters the B-number (local, long distance, or international) where calls are to be forwarded.

Note Centrex subscribers can specify a second forwarding number for in-group calls, but they cannot program this forwarding number via handset. The service provider sets this up at the Centrex subscriber's request.

  - The user receives an appropriate error announcement if the forward-to number is invalid or restricted, or if the feature cannot be activated.
  - If FDT is provisioned, the user hears a confirmation tone for 1 second, followed by the provisioned dial tone, indicating that activation was successful. If FDT is not provisioned, the user hears a success announcement.
  - CFB is now activated, and will stay active until it is deactivated with the appropriate deactivation VSC, or is overridden by the service provider via a CLI command.

CFB Variable Deactivation (CFBVD)

CFB can be deactivated by the service provider. via a CLI command. Alternatively, CFB can be deactivated by user as follows.

Note See the "CFBVA Customization Options" section on page 3-18 for details of the customized feature FDT.

- The user lifts the handset and listens for dial tone.
- The user presses the VSC applicable to CFB deactivation (for example, typically *91 in North America and #40# in China). The VSC values are provisionable by the service provider.
- The user receives an appropriate error announcement if the feature cannot be deactivated.
- If deactivation was successful, and if FDT is provisioned, the user hears a confirmation tone for 1 second, followed by the provisioned dial tone. If FDT is not provisioned, the user hears a success announcement.

CFB is now deactivated, and will stay deactivated until it is activated with the appropriate activation VSC or is overridden by the service provider via a CLI command.

After deactivation, the incoming calls are not forwarded and are completed on the user's phone. If the user has subscribed to and activated call waiting (CW), the system provides the CW tone, and further CW procedures will apply.

CFB Interrogation (CFBI)

CFB interrogation allows a user to check whether CFB is activated to a particular phone. The user performs an interrogation as follows.

Note See the "CFBVA Customization Options" section on page 3-18 for details of customized features SDT and FDT.

- The user lifts the handset and listens for dial tone.
- The user presses the VSC applicable to CFB interrogation (for example, typically *#40* in China). The VSC values are provisionable by the service provider.
- If provisioned for SDT, and if CFB can be interrogated, the system returns the provisioned dial tone. If not provisioned for SDT, no tones are provided.
- The user enters the forward-to number to be interrogated (B-number).

  Note The user can follow the B-number with a # to indicate the end of B-number entry.

  Note If the user enters a digit string that does not match exactly the B-number against which CFB was activated, the interrogation attempt will result in an error announcement.

- The user receives an appropriate error announcement if the CFB feature is not forwarded to the B-number entered, or if the B-number is invalid.

- If FDT is provisioned and the CFB feature is activated to the forward-to number entered, the user hears a confirmation tone for 1 second, followed by the provisioned dial tone.
- If FDT is not provisioned and the CFB feature is activated to the forward-to number entered, the system returns a success announcement.

CFB Invocation

CFB invocation is the actual procedure the system follows to forward the call.

Invalid User Actions

The following user actions are invalid, and the system provides an appropriate error announcement:

- The user enters an invalid directory number (DN) for the B-number.
- During CFB activation, the user enters a B-number that is determined by the system to be a type blocked by provisioning in the NOD-RESTRICT-LIST table. For example, if the nature of dial (NOD) for the B-number is set to EMG (emergency), but calls with NOD=EMG are blocked by provisioning in the NOD-RESTRICT-LIST table, the activation to that B-number will be denied.
- The user tries to activate CFB from a DN that has outgoing calls blocked by the OCB feature, or the user enters a B-number, but calls to that DN are blocked by OCB. For example, the call from the user's phone to the B-number would be a domestic long-distance call, but these calls are blocked by setting K=2 against the OCB feature in the SUBSCRIBER-FEATURE-DATA table.

Note The database tables (NOD-RESTRICT-LIST and SUBSCRIBER-FEATURE-DATA) mentioned in the above list are described in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*. For information on billing records, see the *Cisco BTS 10200 Softswitch Billing Reference Guide*. For information on measurements, see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

- The user tries to activate CFB from or to a DN for which calls are restricted by the COS feature.
- The user tries to activate CFB when already activated (the B-number is not overwritten).
- The user tries to activate CFB to an international DN, but the service provider has blocked forwarding to international DNs. The service provider can block forwarding to international DNs using the international flag in the FEATURE table.
- The user tries to activate CFB to his or her own extension or DN.
- The user tries to deactivate CFB when already deactivated.
- The user interrogates CFB, but enters a digit string that does not match exactly the B-number against which CFB was activated. For example, if CFB was activated with a 5-digit string corresponding to a Centrex extension, and interrogation is attempted using a 10-digit string of the complete DN, the interrogation attempt will result in the applicable announcement. (See the complete list of standard Cisco BTS 10200 announcements in the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.)
- The user tries to interrogate CFB on a fresh system (a system with no entry in the SUBSCRIBER-FEATURE-DATA table). In this case, the user receives the error announcement immediately after entering *#40*. The system does not wait for the user to enter the B-number.

CFB Feature Interactions

This section describes the interaction of other subscriber features with the CFB feature.

- CLIP, CNAM, and CND (caller ID features)—When a call is forwarded, the forwarded-to party receives the DN of the calling party on the caller ID display.
- OCB—The interaction of CFB and OCB depends upon the sequence in which they are activated:
  - If OCB is activated prior to CFB activation—OCB screening is performed on each DN the user enters when attempting to activate CFB. Successful CFB activation depends on the existing OCB K-VALUE and the forward-to DN:

Note If the existing OCB K-VALUE is set to block calls to the forward-to DN, then the system does not allow CFB activation. The user receives an error announcement.

Note If the OCB K-VALUE allows calls to this DN, then the CFB activation process continues. Once the CFB activation attempt to a specific DN is accepted by the system, it is applicable permanently regardless of any future OCB K-VALUE changes. That is, future changes to the OCB K-VALUE have no effect on CFB invocation. CFB to this DN can be deactivated by the user in the normal manner (#40#).

  - If CFB is activated prior to OCB activation—The user can activate the OCB feature, or change the OCB K-VALUE, regardless of the existing CFB feature. However, invocation of OCB depends upon the type of call:

Note User-dialed calls—User-dialed calls can be blocked by OCB (depending on the K-VALUE).

Note Forwarded calls—CFB remains active as originally set up by the user, therefore, calls forwarded by the CFB feature ***cannot*** be blocked using OCB screening.

CW (or CWD)—If both CFB and CW (or CWD) are subscribed to and activated by the user, CW (or CWD) takes precedence. An incoming call to a user already on a call with CW (or CWD) activated will be given the CW (or CWD) tone, and further CW (or CWD) procedures will be applied. The following additional conditions apply:

  - If a user with CW (or CWD) is already involved in a call, the next incoming call is not forwarded. However, any additional incoming calls will be forwarded.
  - If a user with CW (or CWD) has gone off hook but has not yet completed a call or the call is in a ringing state, and there is an incoming call, the call will be forwarded.
- COS—If a call to a DN is restricted by COS screening, CFB cannot be activated or invoked to that DN.
- AR—If Automatic Recall (AR) is used to call a subscriber with CFB feature, the call is not forwarded when the CFB subscriber is off-hook. Instead, the calling subscriber hears the announcement “The user you are calling is busy. The system will check the line for the next 30 minutes, and then you will be notified”. Therefore, CFB feature is not activated when AR is used to call an off-hook CFB subscriber.

For example, consider a situation where Subscriber A uses the AR feature to call Subscriber B, who has the CFB feature activated to forward all calls to C.

Subscriber B is now off-hook, and Subscriber A calls Subscriber B using AR. Here, A's call is not forwarded to C. Instead, Subscriber A hears an announcement informing that Subscriber B is busy.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the CFB provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Call Forwarding No Answer (CFNA)

The BTS 10200 provides the call forwarding no answer (CFNA) feature. CFNA allows a user (the called party) to instruct the network to forward incoming calls that are not answered within a specified number of rings. (Five rings is the default setting, but number of rings is configurable.) A typical forwarding number is voice mail. This service can be used with either rotary or dual tone multifrequency (DTMF) equipped customer premises equipment (CPE).

Note The service provider can provision a parameter that determines the timeout (and thus the number of 6-second rings) before a call is forwarded. The timeout can be set at the feature level (in the Feature table) and at the subscriber level (in the Subscriber Feature Data table), and the setting for the subscriber takes precedence over the setting at the feature level.

The CFNA feature affects the called party in specific ways, depending upon whether the called party phone is on hook or off hook when the call comes in:

- If the forwarding phone is on hook when a call comes in, the phone will ring in the normal manner, and then the call will be forwarded when the CFNA timer runs out.
- If the forwarding phone is off hook when the call comes in, no reminder ring is generated. However, if the user has subscribed to and activated CW (or CWD), the CW (or CWD) treatment will be given first, and then the call will be forwarded after the CFNA timer runs out. The forwarding station is ringing when the CFNA feature is executed, therefore no reminder ring is generated.

Reference documents include:

- LSSGR module FSD 01-02-1401 (GR-580), *Call Forwarding Variable*
- LSSGR Module FSD 01-02-1450 (GR-586), *Call Forwarding Subfeatures*
- LSSGR module FSD 01-02-2200 (GR-1520), *Ring Control*
- ITU-T Q-732.2
- ITU I-252.4

The service provider can provision the CFNA feature to be active immediately on the customer line, or to be activated by the individual subscriber using the handset. The user activates the CFNA feature on the local phone, and enters the forward-to phone number where the user wishes to have the calls forwarded. This forward-to DN is referred to as the B-number. The allowed types of B-numbers are listed in Table 3-4.

Table 3-4 Allowed Types of B-numbers

Subscriber Type	Allowed B-number
POTS	DN, without extensions
Centrex	Public access code + external DN, without extensions
	An extension within the business group

The following conditions apply to the CFNA feature:

- The CFNA feature can be provided to POTS, Centrex, and MLHG subscribers.
- The CFNA feature is in the deactivated mode unless activated by the service provider or subscriber.
- Call forwarding hop scenarios are restricted to a maximum of five hops. The call will be completed on the provisioned maximum number of hops.
- Multiple call forwarding (MCF) is a provisionable option that allows multiple incoming calls to be forwarded by the subscriber at the same time. If a subscriber already has CFNA invoked, additional calls to the subscriber will be forwarded by CFNA based on the MCF flag. If the MCF flag is turned off, only one CFNA invocation is allowed.

The CFNA feature is composed of four associated features, which are described in the sections that follow:

- CFNA Variable Activation (CFNAVA), page 3-24
- CFNA Variable Deactivation (CFNAVD), page 3-27
- CFNA Interrogation (CFNAI), page 3-27
- CFNA Invocation, page 3-28

Additional information about this feature is covered in the following sections:

- Invalid User Actions, page 3-28
- CFNA Feature Interactions, page 3-29
- Feature Provisioning Commands, page 3-30

CFNA Variable Activation (CFNAVA)

This section discusses how the service provider can customize CFNAVA, and the CFNAVA procedures available to the handset user.

Blocking Call Forwarding to Certain Types of DNs

The service provider can block call forwarding to certain types of DNs by provisioning the nature of dial (NOD) parameter for the call-forwarding features (CFU, CFB, CFNA, and CFC) in the NOD Restrict List (nod-restrict-list) table. For example, if you provision NOD=TOLL-FREE and NOD=EMG in the nod-restrict-list table, the system will not allow call-forwarding to DNs of those types.

Caution If you want to block call-forwarding to an emergency (EMG) DN, such as 911, you must provision NOD=EMG for the call-forwarding features (CFU, CFB, CFNA, and CFC) in the NOD-RESTRICT-LIST. This is necessary to comply with the rule in Telcordia document GR-580, which says that 911 should not be a permitted “forward to” number.

Tip To provision the CFNA feature, see the CFNA provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

CFNAVA Customization Options

The behavior of CFNAVA can be customized using the following provisionable options. The detailed provisioning steps for these options are provided in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

- Courtesy call (CC)—The CC flag controls the delivery of a courtesy call while activating CFNA. Although this option can be provisioned, as a practical matter it usually is not provided with CFNA service in most markets.
- Second stage dial tone (SDT)—The SDT flag controls the delivery of a dial tone after the subscriber enters the VSC for activation or interrogation of CFNA. The permitted values for this flag are:
  - NO_TONE
  - DIAL_TONE
  - STUTTER_DIAL_TONE
  - CONFIRMATION_TONE
  - CONFIRMATION_DIAL_TONE

Note For SIP phone subscribers, the SDT parameter has no effect. The SDT option is available through the dial plan in the SIP phone.

- Final stage dial tone (FDT)—The FDT flag controls the system response to a successful activation, deactivation or interrogation of CFNA by the subscriber. If FDT is not provisioned, the system provides a success announcement. The permitted values for this flag are the same as for the SDT flag.

Note For SIP phone subscribers, only the success announcements will be provided. The confirmation tone and dial tone will not be provided, even if the FDT flag is set.

- Multiple call forwarding (MCF)—When provisioned as Y, MCF allows multiple incoming calls to be forwarded by the subscriber at the same time. If a subscriber already has CFNA invoked, additional calls to the subscriber will be forwarded by CFNA based on the MCF flag. If the MCF flag is set to N, only one CFNA invocation is allowed.
- International call forwarding (INTL)—When the INTL flag is set to N, forwarding to an international number is not allowed. When INTL is set to Y, the system checks for other restrictions on international calls, and allows forwarding if there are no other restrictions provisioned for the call type and calling number. (Other provisionable restrictions on international calling can be based on the nature of dial (NOD) and the subscriber feature data.)

Detailed information on how to set these parameters is provided in the following documents:

Detailed information on how to set these parameters is provided in the following documents:

- The “Valid Features” appendix in the *Cisco BTS 10200 Softswitch Command Line Interface Guide for Call Processing* lists all of the TYPE/VALUE pairs that are valid for each feature, including FDT, SDT, CC, and so forth.

- The "Feature Profile Base" section in the "Valid Features" appendix of the *Cisco BTS 10200 Softswitch Command Line Interface Guide for Call Processing* provides descriptions of the TYPE/VALUE pairs.
- The CFNA provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide* lists the provisioning commands to use with these parameters.

CFNAVA Handset Procedures

CFNA can be activated by the service provider or by the individual user. The procedures are as follows:

- CFNA can be activated permanently at subscription time by the service provider. The service provider provisions the forward-to DN as requested by the subscriber. When the phone is not answered, calls made to the subscriber's line will be forwarded to the single forward-to number that was provisioned.
- CFNA can be activated by the user as follows.

Note See the "CFNAVA Customization Options" section on page 3-25 for details of customized features CC, SDT, and FDT.

  - The user lifts the handset and listens for dial tone.
  - The user presses the VSC applicable to CFNA activation (for example, typically *92 in North America and *41* in China). The VSC values are provisionable by the service provider.
  - If provisioned for SDT, and if CFNA can be activated, the system returns the provisioned dial tone.
  - The user enters the B-number (local, long distance, or international) where calls are to be forwarded.

Note Centrex subscribers can specify a second forwarding number for in-group calls, but they cannot program this forwarding number via handset. The service provider sets this up at the Centrex subscriber's request.

  - The user receives an appropriate error announcement if the forward-to number is invalid or restricted, or if the feature cannot be activated.
  - If the feature can be activated to the forward-to number entered, the system returns a confirmation tone and attempts to place a courtesy call to the forward-to number (if provisioned for CC).
  - If the forwarded-to party answers the courtesy call (when CC is provisioned as ANS), or if CC is provisioned as NOANS, the CFNA feature is activated.

Note When CC is provisioned for ANS, and if the forwarded-to line is busy or does not answer, the CFNA feature is not activated. The user can still activate CFNA by repeating the activation procedure within 2 minutes of the first attempt. No courtesy call is set up during the second attempt. The user hears a confirmation tone. If more than 2 minutes elapse before the second attempt, the second attempt is treated as a first attempt.

- If FDT is provisioned, the user hears a confirmation tone for 1 second, followed by the provisioned dial tone, indicating that activation was successful. If FDT is not provisioned, the user hears a success announcement.
- CFNA is now activated, and will stay active until it is deactivated using the appropriate deactivation VSC, or is overridden by the service provider via a CLI command.

CFNA Variable Deactivation (CFNAVD)

CFNA can be deactivated by the service provider via a CLI command. Alternatively, CFNA can be deactivated by the individual user as follows.

Note See the "CFNAVA Customization Options" section on page 3-25 for details of the customized feature FDT.

- The user lifts the handset and listens for dial tone.
- The user presses the VSC applicable to CFNA deactivation (for example, typically *93 in North America and #41# in China). The VSC values are provisionable by the service provider.
- The user receives an appropriate error announcement if the feature cannot be deactivated.
- If deactivation was successful, and if FDT is provisioned, the user hears a confirmation tone for 1 second, followed by the provisioned dial tone. If FDT is not provisioned, the user hears a success announcement.

CFNA is now deactivated, and will stay deactivated until it is activated using the appropriate activation VSC or is overridden by the service provider via a CLI command.

After deactivation, the incoming calls are not forwarded and are completed on the user's phone.

CFNA Interrogation (CFNAI)

CFNA interrogation allows a user to check whether CFNA is activated to a particular phone. The user performs an interrogation as follows.

Note See the "CFNAVA Customization Options" section on page 3-25 for details of customized features SDT and FDT.

- The user lifts the handset and listens for dial tone.
- The user presses the VSC applicable to CFNA interrogation (for example, typically *#41* in China). The VSC values are provisionable by the service provider.
- If provisioned for SDT, and if CFNA can be interrogated, the system returns a confirmation tone for one second and then the provisioned dial tone. If not provisioned for SDT, no tones are provided.
- The user enters the forward-to number to be interrogated (B-number).

Note The user can follow the B-number with a # to indicate the end of B-number entry.

Note If the user enters a digit string that does not match exactly the B-number against which CFNA was activated, the interrogation attempt will result in an error announcement.

- The user receives an appropriate error announcement if the CFNA feature is not forwarded to the B-number entered or if the B-number is invalid.
- If FDT is provisioned and the CFNA feature is activated to the forward-to number entered, the user hears a confirmation tone for one second, followed by the provisioned dial tone.
- If FDT is not provisioned and the CFNA feature is activated to the forward-to number entered, the system returns a success announcement.

CFNA Invocation

CFNA invocation is the actual procedure the system follows to forward the call.

Invalid User Actions

The following user actions are invalid, and the system provides an appropriate error announcement:

- The user enters an invalid directory number (DN) for the B-number.
- During CFNA activation, the user enters a B-number that is determined by the system to be a type blocked by provisioning in the NOD-RESTRICT-LIST table. For example, if the nature of dial (NOD) for the B-number is set to EMG (emergency), but calls with NOD=EMG are blocked by provisioning in the NOD-RESTRICT-LIST table, the activation to that B-number will be denied.
- The user tries to activate CFNA from a DN that has outgoing calls blocked by the OCB feature, or the user enters a B-number, but calls to that DN are blocked by OCB. For example, the call from the user's phone to the B-number would be a domestic long-distance call, but these calls are blocked by setting K=2 against the OCB feature in the SUBSCRIBER-FEATURE-DATA table.

Note The database tables (NOD-RESTRICT-LIST and SUBSCRIBER-FEATURE-DATA) mentioned in the above list are described in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*. For information on billing records, see the *Cisco BTS 10200 Softswitch Billing Reference Guide*. For information on measurements, see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

- The user tries to activate CFNA from or to a DN for which calls are restricted by the COS feature.
- The user tries to activate CFNA when already activated (the B-number is not overwritten).
- The user tries to activate CFNA to an international DN, but the service provider has blocked forwarding to international DNs. The service provider can block forwarding to international DNs using the international flag in the FEATURE table.
- The user tries to activate CFNA to his or her own extension or DN.
- The user tries to deactivate CFNA when already deactivated.
- The user interrogates CFNA, but enters a digit string that does not match exactly the B-number against which CFNA was activated. For example, if CFNA was activated with a 5-digit string corresponding to a Centrex extension, and interrogation is attempted using a 10-digit string of the

complete DN, the interrogation attempt will result in the applicable announcement. (See the complete list of standard Cisco BTS 10200 announcements in the *Cisco BTS 10200 Softswitch Provisioning Guide*.)

- The user tries to interrogate CFNA on a fresh system (a system with no entry in the SUBSCRIBER-FEATURE-DATA table). In this case, the user receives the error announcement immediately after entering *#41*. The system does not wait for the user to enter the B-number.

CFNA Feature Interactions

This section describes the interaction of other subscriber features with the CFNA feature.

- CLIP, CNAM, and CND (caller ID features)—When a call is forwarded, the forwarded-to party receives the DN of the calling party on the caller ID display.
- COS—If a call to a DN is restricted by COS screening, CFNA cannot be activated or invoked to that DN.
- OCB—The interaction of CFNA and OCB depends upon the sequence in which they are activated:
  - If OCB is activated prior to CFNA activation—OCB screening is performed on each DN the user enters when attempting to activate CFNA. Successful CFNA activation depends on the existing OCB K-VALUE and the forward-to DN:

Note If the existing OCB K-VALUE is set to block calls to the forward-to DN, then the system does not allow CFNA activation. The user receives an error announcement.

Note If the OCB K-VALUE allows calls to this DN, then the CFNA activation process continues. Once the CFNA activation attempt to a specific DN is accepted by the system, it is applicable permanently regardless of any future OCB K-VALUE changes. That is, future changes to the OCB K-VALUE have no effect on CFNA invocation. CFNA to this DN can be deactivated by the user in the normal manner (#41#).

  - If CFNA is activated prior to OCB activation—The user can activate the OCB feature, or change the OCB K-VALUE, regardless of the existing CFNA feature. However, invocation of OCB depends upon the type of call:

Note User-dialed calls—User-dialed calls can be blocked by OCB (depending on the K-VALUE).

Note Forwarded calls—CFNA remains active as originally set up by the user, therefore, calls forwarded by the CFNA feature ***cannot*** be blocked using OCB screening.

- There is an interaction when a Centrex subscriber has all three of the following features assigned and active:
  1. Call hold—CHD.
  2. Call waiting—CW or CIDCW or both.
  3. Call forwarding on no answer—CFNA, VM (or VMA), or any combination of these.

For information on this interaction, see the "CHD with CW/CIDCW and CFNA/VM/VMA" section on page 3-70.

- If CHD is assigned to the subscriber along with CFNA (CFNA active), the following interaction occurs.
  - A (the subscriber) and B are on an active call.
  - C calls A.
  - C hears a busy tone and is not connected. The call from C is not forwarded by the CFNA feature.
- CW or CWD—If both CFNA and CW (or CWD) are subscribed to and activated by the user, the interaction is as follows. If the user is on an active call when a new call comes in, the CW (or CWD) tone will be played. If the user presses the Flash button or hookswitch before the CFNA timer runs out, the user will be connected to the new call, and the call will proceed according to the CW (or CWD) feature. If the user takes no action, and the CFNA timer runs out, the waiting call will be forwarded per the CFNA procedure.

  Several provisionable parameters can affect the processing of this call.
  - The CW timeout is based on a switch-wide parameter, NO-ANSWER-TMR in the ca-config table (default 185 seconds). There is also a parameter, START-NO-ANSWER-TMR in the ca-config table, to specify whether NO-ANSWER-TMR is to be started or not; default is N.

    The CFNA timeout is provisioned via the TYPE1=TO parameter in the Feature table (default 30 seconds).
  - If Subscriber A has the default timer settings (that is, CFNA TO=30 seconds and NO-ANSWER-TIMER=185 seconds), and has the START-NO-ANSWER-TMR parameter set to Y (not the default), the call is processed as follows:

    [1] A calls B, B answers.

    [2] C calls A, A hears the CW tone, C hears ring tone.

    [3] If A does not attempt to answer the waiting call (C), and CFNA times out (30 seconds), C is forwarded according to normal CFNA procedures.

    However, if the CFNA timeout (TO) is set to a value *greater than* NO-ANSWER-TMR, when NO-ANSWER-TMR expires, C is disconnected and hears a busy tone, and CFNA is cancelled.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the CFNA provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Call Forwarding Combination (CFC)

The system supports a set of vertical service codes (VSCs) to activate, deactivate, and interrogate Call Forwarding Combination (CFC). Once activated, CFC forwards incoming calls to the subscriber when the subscriber is either busy or does not answer. This feature combines the functionality of CFB and CFNA.

The forward-to DN is referred to as the B-number. The allowed types of B-numbers are listed in Table 3-5.

Table 3-5 Allowed Types of B-numbers

Subscriber Type	Allowed B-number
POTS	DN, without extensions
Centrex	Public access code + external DN, without extensions
	An extension within the business group

The following conditions apply to the CFC feature:

- The CFC feature can be provided to POTS, Centrex, and MLHG subscribers.
- The CFC feature is in the deactivated mode unless activated by the service provider or subscriber.
- Call forwarding hop scenarios are restricted to a maximum of five hops. The call will be completed on the provisioned maximum number of hops.
- Multiple call forwarding (MCF) is a provisionable option that allows multiple incoming calls to be forwarded by the subscriber at the same time. If a subscriber already has CFC invoked, additional calls to the subscriber will be forwarded by CFC based on the MCF flag. If the MCF flag is turned off, only one CFC invocation is allowed.

Vertical Service Codes for CFC

The values of the VSCs are provisionable. Typical VSC examples for the CFC subfeatures are as follows:

- *68—CFC_ACT (CFC Activation without change of forward-to DN)
- *88—CFC_DEACT (CFC Deactivation)
- *201—CFC_DN_CHG_ACT (CFC Activation with change of forward-to DN)
- *202—CFCI_NO_DN_VRFY (CFC Interrogation without forward-to DN verification)
- *203—CFCI (CFC Interrogation with forward-to DN verification)

Blocking Call Forwarding to Certain Types of DNs

The service provider can block call forwarding to certain types of DNs by provisioning the nature of dial (NOD) parameter for the call-forwarding features (CFU, CFB, CFNA, and CFC) in the NOD Restrict List (nod-restrict-list) table. For example, if you provision NOD=TOLL-FREE and NOD=EMG in the nod-restrict-list table, the system will not allow call-forwarding to DNs of those types.

Caution If you want to block call-forwarding to an emergency (EMG) DN, such as 911, you must provision NOD=EMG for the call-forwarding features (CFU, CFB, CFNA, and CFC) in the NOD-RESTRICT-LIST. This is necessary to comply with the rule in Telcordia document GR-580, which says that 911 should not be a permitted "forward to" number.

Detailed Feature Description

The CFC feature is composed of six associated features, which are described in the sections that follow:

- CFC Activation (CFC_ACT)
- CFC Deactivation (CFC_DEACT)
- CFC Activation with Directory Number Change (CFC_DN_CHG_ACT)
- CFC Interrogation with No Directory Number Verification (CFCI_NO_DN_VRFY)
- CFC Interrogation (CFCI)
- CFC Invocation (CFC)

Additional information about this feature is covered in the following sections:

- Flags Applicable to CFC Activation and Deactivation Subfeatures, page 3-34
- Invalid User Actions, page 3-37
- CFC Feature Interactions, page 3-38
- Feature Provisioning Commands, page 3-39

CFC Activation (CFC_ACT)

CFC activation allows the end user to activate CFC to a pre-defined DN (which was set up when provisioning the feature). However, the end user cannot change the DN via this feature.

To activate CFC, the subscriber dials the access code for activation. If the final dial tone parameter (FDT) is provisioned, the subscriber hears the provisioned dial tone if the feature is successfully activated. If the feature is not successfully activated, the subscriber hears a reorder tone, or an announcement, if the announcements are provisioned.

If the feature is already active, the subscriber hears a stutter dial tone confirming that the feature is active.

While activating CFC, the pre-defined DN is validated. To be valid, the DN must conform to the dial-plan provisioned in the Call Agent (CA).

Activating CFC has some limitations, including:

- The subscriber cannot activate CFC if the pre-defined DN is the subscriber's own DN or extension.
- The subscriber cannot activate CFC if the pre-defined DN is blocked by Outgoing Call Barring (OCB).

- The subscriber cannot activate CFC if the pre-defined DN has a call-type which is blocked by the CFC nod-restrict-list. Where applicable, all CFC features treat the nod-restrict list as a black list.

The pre-defined DN can be a speed code. However, to be valid, the translated DN must conform to the dial-plan provisioned in the CA.

For CENTREX subscribers, the pre-defined DN can be an extension or a PAC followed by a DN.

CFC Deactivation (CFC_DEACT)

CFC deactivation allows the end user to deactivate the CFC feature. However, even if the feature is deactivated, the forwarding DN for the subscriber is preserved.

To deactivate CFC, the subscriber dials the access code for deactivation. If the FDT parameter is provisioned, the subscriber hears the provisioned dial tone if the feature is successfully deactivated. If the feature is not successfully deactivated, the subscriber hears a reorder tone or an announcement, if announcements are provisioned.

If the feature is already inactive, the subscriber hears a stutter dial tone confirming that the feature is inactive.

For CFC deactivation, the DN validity is not checked. The feature simply deactivates CFC without any checks.

CFC Activation with Directory Number Change (CFC_DN_CHG_ACT)

CFC with directory number change enables the subscriber to activate CFC to a user-defined remote DN, and the end user can change the DN via this feature.

To activate this feature, the subscriber begins by dialing an access code for activation. If the second dial tone parameter (SDT) is provisioned, the subscriber hears the provisioned dial tone, and enters the Forwarding DN. If the FDT parameter is provisioned, the subscriber hears the provisioned dial tone if the feature is successfully activated. If the feature is not successfully activated, the subscriber hears a reorder tone or an announcement, if announcements are provisioned.

If the feature is already active, the subscriber hears a stutter dial tone confirming that the feature is active.

While activating the feature, the user-defined DN is checked for validity. To be valid, the DN must conform to the dial-plan provisioned in the CA.

Activating CFC with Directory Number Change has some limitations, including:

- The subscriber cannot activate CFC if the user-defined DN is the subscriber's own DN or extension.
- The subscriber cannot activate CFC is the user-defined DN is blocked by OCB.
- The subscriber cannot activate CFC is the user-defined DN has a call-type which is blocked by the CFC nod-restrict-list. Where applicable, all CFC features treat the nod-restrict list as a black list.

The user-defined DN can be a speed code. However, to be valid, the translated DN should conform to the dial-plan provisioned in the CA. The feature stores the translated DN as the forwarding number in the database.

For CENTREX subscribers, the pre-defined DN can be an extension or a PAC followed by a DN. If CFC is activated with an extension, the feature stores that extension as the forwarding number in the database.

CFC Interrogation with No Directory Number Verification (CFCI_NO_DN_VRFY)

CFC Interrogation with no directory number verification enables the subscriber to verify (or interrogate) whether CFC is active on the subscriber's line or not.

To use the feature, the subscriber dials a star code. If the FDT parameter is provisioned and CFC is active, the subscriber hears the provisioned dial tone. If CFC is not active, the subscriber hears a reorder tone or an announcement, if announcements are provisioned.

CFC Interrogation (CFCI)

CFC interrogation enables the subscriber to verify (or interrogate) whether CFC is active on the subscriber's line to a certain DN or not.

To use the feature, the subscriber dials the access code for interrogation. If the SDT parameter is provisioned, the subscriber hears the provisioned dial tone, and enters the DN against which to perform the verification. If the FDT parameter is provisioned, and if CFC is active to that DN, the subscriber hears the provisioned dial tone. If CFC is not active, or active to a different DN, the subscriber hears a reorder tone or an announcement, if announcements are provisioned.

The verification is done against the exact DN stored in the database for CFC. The feature does not translate or do any conversion before comparing the numbers (like extension to a DN, or adding a country code if the number is not fully specified by the user, or converting from a speed code to a DN).

CFC Invocation (CFC)

The CFC invocation feature forwards a call coming to the subscriber when the subscriber is either busy or does not answer. CFC checks the nod-restrict-list check for call-types blocked on CFC. Provision the nod-restrict-list with the same fname as CFC.

CFC is considered deactivated unless explicitly activated by the subscriber.

The following flags are provisionable in the feature table, and affect the forwarding behavior of CFC:

- Multiple call forwarding (MCF)—Setting the MCF flag to Y (Yes) allows multiple calls to be forwarded at the same time. Setting the MCF flag to N (No) allows the subscriber to have only one busy or one no-answer call forwarded at a time.
- Timeout (TO)—The TO flag is used for the no-answer timeout for CFC. The default value is 30 seconds.

Flags Applicable to CFC Activation and Deactivation Subfeatures

There are three optional TYPE-VALUE pairs to configure for CFC subfeatures in the feature table. The TYPE-VALUE pairs correspond to the SDT, FDT and CC flags. This section describes the feature behavior based on these flags.

Table 3-6 shows which flags are applicable to each feature, and lists the default values for the flags.

Table 3-6 Flags for CFC Activation and Deactivation Subfeatures

Feature	Flag	Default Value(s)
CFC_DN_CHG_ACT **Note** The INTL flag is also applicable to this feature (default N).	SDT	DIAL_TONE
	FDT	STUTTER_DIAL_TONE
	CC	N
CFC_DEACT	SDT	Feature does not need the flag when executed.
	FDT	STUTTER_DIAL_TONE
	CC	Feature does not need the flag when executed.
CFC_ACT	SDT	Feature does not need the flag when executed.
	FDT	STUTTER_DIAL_TONE
	CC	Feature does not need the flag when executed.
CFCI_NO_DN_VRFY	SDT	Feature does not need the flag when executed.
	FDT	STUTTER_DIAL_TONE
	CC	Feature does not need the flag when executed.
CFCI	SDT	DIAL_TONE
	FDT	STUTTER_DIAL_TONE
	CC	Feature does not need the flag when executed.

TYPE-VALUE Pair 1—SDT

The first TYPE-VALUE pair for the second dial tone (SDT) is:

```
TYPEn=SDT;
VALUEn=[NO_TONE|DIAL_TONE|STUTTER_DIAL_TONE|CONFIRMATION_TONE|CONFIRMATION_DIAL_TONE]
```

If provisioned, this pair specify the tone to play just after the subscriber dials the VSC.

The following tones play based on the values set:

- If the VALUE is set to NO_TONE, no tones play.
- If VALUE is set to DIAL_TONE, the dial tone plays.
- If VALUE is set to STUTTER_DIAL_TONE, a stutter dial tone plays.
- If the VALUE is set to CONFIRMATION_DIAL_TONE, a confirmation, followed by the dial tone, plays.
- If the VALUE is set to CONFIRMATION_TONE, a confirmation tone is played.

Note For SIP phone subscribers, the SDT parameter has no effect. The SDT option is available through the dial plan in the SIP phone.

TYPE-VALUE Pair 2—FDT

The second TYPE-VALUE pair for final dial tone (FDT) is:

```
TYPEn=FDT;
VALUEn=[NO_TONE|DIAL_TONE|STUTTER_DIAL_TONE|CONFIRMATION_TONE|CONFIRMATION_DIAL_TONE]
```

If provisioned, the pair dictates what tone to play after the subscriber successfully activates or deactivates the feature.

The following tones play based on the values set:

- If the VALUE is set to NO_TONE and if the announcement server is provisioned, an announcement plays.
- If VALUE is set to DIAL_TONE, a dial tone plays.
- If VALUE is set to STUTTER_DIAL_TONE, a stutter dial tone plays.
- If the VALUE is set to CONFIRMATION_DIAL_TONE, a confirmation, followed by the dial tone, plays.
- If the VALUE is set to CONFIRMATION_TONE, a confirmation tone is played.

Note For SIP phone subscribers, only the success announcements will be provided. The confirmation tone and dial tone will not be provided, even if the FDT flag is set.

TYPE-VALUE Pair 3—CC

The third TYPE-VALUE pair is:

```
TYPEn=CC;
VALUEn=[ANS|NOANS|N]
```

If provisioned, the pair above dictates the feature behavior after the subscriber successfully activates the CFC_DN_CHG_ACT feature.

Note This flag is applicable to only this feature.

The feature behaviors depend on the following values:

- If the VALUE is set to ANS, a courtesy call is placed to a forwarding number entered by the user; CFC is activated to that number only when the remote party answers the call. If the remote party does not answer, or if the subscriber hangs up, the subscriber has two minutes to dial the CFC_DN_CHG_ACT access code, followed by the same number, to force CFC activation to that number. At this point, no courtesy call is placed to the number, and CFC is activated.
- If the value is set to NOANS, a courtesy call is placed to the forwarding number entered by the user, but the remote party need not answer the call to activate CFC. CFC is activated whether the courtesy call is successful, or whether the remote party answered.

- If the VALUE is set to N, no courtesy call is placed when the subscriber successfully activates CFC_DN_CHG_ACT. Instead, the feature looks up the FDT flag for the appropriate treatment.

Additional Provisioning Details

To view a list of these feature options for CFC in the *Cisco BTS 10200 Softswitch CLI Database*, use the **show feature-profile-base fname=cfc** CLI command.To provision the CFU feature, see t he CFC provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Invalid User Actions

The following user actions are invalid, and the system provides an appropriate error announcement:

- The user enters an invalid directory number (DN) for the B-number.
- The user tries to activate CFC (with CC set to ANS) for the second time within a 2-minute interval to a DN which is different from the one used in the first attempt. (In addition, the history associated with the first attempt will be removed.)
- During CFC activation, the user enters a B-number that is determined by the system to be a type blocked by provisioning in the NOD-RESTRICT-LIST table. For example, if the nature of dial (NOD) for the B-number is set to EMG (emergency), but calls with NOD=EMG are blocked by provisioning in the NOD-RESTRICT-LIST table, the activation to that B-number will be denied.
- The user tries to activate CFC from a DN that has outgoing calls blocked by the OCB feature, or the user enters a B-number, but calls to that DN are blocked by OCB. For example, the call from the user's phone to the B-number would be a domestic long-distance call, but these calls are blocked by setting K=2 against the OCB feature in the SUBSCRIBER-FEATURE-DATA table.

Note The database tables (NOD-RESTRICT-LIST and SUBSCRIBER-FEATURE-DATA) mentioned in the above list are described in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*. For information on billing records, see the *Cisco BTS 10200 Softswitch Billing Reference Guide*. For information on measurements, see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

- The user tries to activate CFC from or to a DN for which calls are restricted by the COS feature.
- The user tries to activate CFC when already activated (the B-number is not overwritten).
- The user tries to activate CFC to an international DN, but the service provider has blocked forwarding to international DNs. The service provider can block forwarding to international DNs using the international flag in the FEATURE table.
- The user tries to activate CFC to his or her own extension or DN.
- The user tries to deactivate CFC when already deactivated.
- The user interrogates CFC, but enters a digit string that does not match exactly the B-number against which CFC was activated. For example, if CFC was activated with a 5-digit string corresponding to a Centrex extension, and interrogation is attempted using a 10-digit string of the complete DN, the interrogation attempt will result in an error announcement. (See the complete list of standard Cisco BTS 10200 announcements in the *Cisco BTS 10200 Softswitch Provisioning Guide*.)
- The user tries to interrogate CFC on a fresh system (a system with no entry in the SUBSCRIBER-FEATURE-DATA table). In this case, the user receives the error announcement immediately after entering the interrogation code (for example, *68). The system does not wait for the user to enter the B-number

CFC Feature Interactions

This section describes the interaction of other subscriber features with the CFC feature.

- CLIP, CNAM, and CND (caller ID features)—When a call is forwarded, the forwarded-to party receives the DN of the calling party on the caller ID display.
- OCB—The interaction of CFC and OCB depends upon the sequence in which they are activated:
  - If OCB is activated prior to CFC activation—OCB screening is performed on each DN the user enters when attempting to activate CFC. Successful CFC activation depends on the existing OCB K-VALUE and the forward-to DN:

Note If the existing OCB K-VALUE is set to block calls to the forward-to DN, then the system does not allow CFC activation. The user receives an error announcement.

Note If the OCB K-VALUE allows calls to this DN, then the CFC activation process continues. Once the CFC activation attempt to a specific DN is accepted by the system, it is applicable permanently regardless of any future OCB K-VALUE changes. That is, future changes to the OCB K-VALUE have no effect on CFC invocation. CFC to this DN can be deactivated by the user in the normal manner (#57#).

  - If CFC is activated prior to OCB activation—The user can activate the OCB feature, or change the OCB K-VALUE, regardless of the existing CFC feature. However, invocation of OCB depends upon the type of call:

Note User-dialed calls—User-dialed calls can be blocked by OCB (depending on the K-VALUE).

Note Forwarded calls—CFC remains active as originally set up by the user, therefore, calls forwarded by the CFC feature ***cannot*** be blocked using OCB screening.

- **CFC_ACT and COS**: If a call to a DN is restricted by COS screening, CFC cannot be activated or invoked to that DN.
- **CFC Activation/Deactivation and Speed Call/Abbreviated Dial:** Subscribers can set their speed call to the CFC Activation/Deactivation access codes. For example, with One-Digit Speed Call, the subscriber can set the speed call for digit "2" to map to "*68" which can be the CFC Activation access code.
- **CFC Activation and OCB:** CFC Activation to a DN blocked by outgoing call barring (OCB) results in a re-order tone or announcement.
- **CFC Activation with DN Change and OCB:** CFC Activation with DN Change to a DN blocked by OCB results in a re-order tone or announcement.
- **CFC and OCB:** Calls are not forwarded by CFC to DNs blocked by OCB for the subscriber.
- **CFC and CFU:** If a subscriber has both CFC and call forwarding unconditional (CFU) assigned and active, incoming calls are forwarded by CFU.
- **CFC and CFB:** If a subscriber has both CFC and CFB assigned and active, incoming calls on which the subscriber is busy are forwarded by CFB.

- **CFC and CFB, CFB is deactivated:** If a subscriber has both CFC and CFB assigned, and CFC active and CFB inactive, incoming calls on which the subscriber is busy are forwarded by CFC.
- **CFC and CFNA:** If a subscriber has both CFC and CFNA assigned and active, incoming calls on which the subscriber does not answer are forwarded by CFNA.
- **CFC and CFNA, CFNA is deactivated:** If a subscriber has both CFC and CFNA assigned, and CFC active and CFNA inactive, incoming calls on which the subscriber does not answer are forwarded by CFC.
- **CFC and VM:** If a subscriber has both CFC and voice mail (VM) assigned and active, and the subscriber is either busy or does not answer, the call is forwarded by CFC.
- **CFC and VM, CFC deactivated:** If a subscriber has both CFC and VM assigned but CFC is deactivated and VM is active, and the subscriber is either busy or does not answer, the call is terminated to VM.
- **CFC and VMA:** If a subscriber has both CFC and VMA assigned and active, the call is terminated to VM.

Note Voice Mail (VM) enables the subscriber to forward calls to voice mail when the subscriber is busy or does not answer the phone. Voice Mail Always (VMA) enables the subscriber to forward all calls to voice mail, regardless of the state of the phone.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the CFC provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Call Waiting Features

Call waiting features notify a called party, who is already on an active call, that another incoming call is being attempted on the line. The called party has the option of answering or ignoring the new incoming call. This section describes four call waiting features:

- Call Waiting (CW), page 3-40
- Cancel Call Waiting (CCW), page 3-42
- Calling Identity Delivery on Call Waiting (CIDCW), page 3-43
- Call Waiting Deluxe (CWD), page 3-46

Note CW, CCW, and CIDCW are typically bundled as an integral part of a service package.

Limitations

If your network uses an ISUP variant other than ANSI ISUP, the system supports CWD, but not CW or CIDCW.

Call Waiting (CW)

The BTS 10200 supports the call waiting (CW) feature as specified in LSSGR module FSD 01-02-1201 (TR-NWT-000571), *Call Waiting*.

CW informs a busy station that another call is waiting through the application of a 300 ms, 440 Hz tone. Ten seconds after the initial tone, a second tone is applied if the waiting call has not been answered. To answer the waiting call and place the original call on hold, the user presses the **Flash** button or **hookswitch**. A subsequent flash returns the user to the original call. Additional flashes can be used to toggle between the two calls as long as they are both still connected. The waiting call hears ringing until it is answered.

When a waiting call is accepted, there are two active sessions. To end the currently active session, the user goes on hook. The user's phone will then ring to indicate that the other caller is still holding. The user can pick up the phone to resume that session.

If a media gateway-connected handset is off hook, but no active call yet exists (that is, receiving a dial tone), then an incoming call receives a station busy tone and CW is not activated.

Only one instance of CW can be active for a given subscriber line at any given time. Thus, if a subscriber line were involved in both an active call and a waiting call, then an additional incoming call attempt results in the caller receiving a busy tone or being forwarded (CFB). The user involved in the CW call is not aware of the additional incoming call attempt.

Note For information on the CIDCW feature, see the "Calling Identity Delivery on Call Waiting (CIDCW)" section on page 3-43.

CW, CIDCW, and CWD interaction—CWD has a higher precedence than CIDCW, and CIDCW has a higher precedence than CW.

CW Activation

CW has multiple activation options as follows:

- Activated permanently at subscription time by service provider.

Tip When CW and CIDCW are first provisioned by the service provider, they are active immediately by default. To assign these features in the deactivated state, configure the subscriber-feature-data table for that subscriber to make CW and CIDCW deactivated.

- The feature can be activated by the individual user if the service provider has assigned the call waiting deluxe activation (CWDA) feature. The steps are as follows.
  - The user lifts the handset, and listens for a dial tone.
  - The user presses the activation VSC (for example, ***58**). If CW can be activated, the system returns a success announcement. An error announcement, indicating the type of error, is given if activation is unsuccessful.

    Note If CW is already activated on this subscriber line, the activation attempt is accepted and processed as a new activation attempt.

  - CW is now activated, and will stay active until it is deactivated (see "CW Deactivation" below).

CW Deactivation

CW deactivation options are as follows:

- Service provider deactivation at user request.
- The feature can be deactivated by the individual user if the service provider has assigned the call waiting deluxe deactivation (CWDD) feature. The steps are as follows.
  - The user lifts the handset and listens for a dial tone.
  - The user presses the deactivation VSC (for example, ***59**). A success announcement is given on a successful deactivation. An error announcement, indicating the type of error, is given if deactivation is unsuccessful.

Note If CW is already deactivated on this subscriber line, the deactivation attempt is accepted and processed as a new deactivation attempt.

  - CW is now deactivated, and will stay inactive until it is activated (see "CW Activation" above).

CW Feature Interactions

- CFNA—If both CW and CFNA are subscribed to and activated by the user, the interaction is as follows. If the user is on an active call when a new call comes in, the CW (or CWD) tone will be played. If the user presses the Flash button or hookswitch before the CFNA timer runs out, the user will be connected to the new call, and the call will proceed according to the CW (or CWD) feature. If the user takes no action, and the CFNA timer runs out, the waiting call will be forwarded per the CFNA procedure.

  Several provisionable parameters can affect the processing of this call.

  - The CW timeout is based on a switch-wide parameter, NO-ANSWER-TMR in the ca-config table (default 185 seconds). There is also a parameter, START-NO-ANSWER-TMR in the ca-config table, to specify whether NO-ANSWER-TMR is to be started or not; default is N.

    The CFNA timeout is provisioned via the TYPE1=TO parameter in the Feature table (default 30 seconds).

  - If Subscriber A has the default timer settings (that is, CFNA TO=30 seconds and NO-ANSWER-TIMER=185 seconds), and has the START-NO-ANSWER-TMR parameter set to Y (not the default), the call is processed as follows:

    [1] A calls B, B answers.

    [2] C calls A, A hears the CW tone, C hears ring tone.

    [3] If A does not attempt to answer the waiting call (C), and CFNA times out (30 seconds), C is forwarded according to normal CFNA procedures.

    However, if the CFNA timeout (TO) is set to a value *greater than* NO-ANSWER-TMR, when NO-ANSWER-TMR expires, C is disconnected and hears a busy tone, and CFNA is cancelled.

- VM—If both CW and VM are subscribed to and activated by the user, the following scenarios apply. Several provisionable parameters can affect the processing of this call.
  - The CW timeout is based on a switch-wide parameter, NO-ANSWER-TMR in the ca-config table (default 185 seconds). There is also a parameter, START-NO-ANSWER-TMR in the ca-config table, to specify whether NO-ANSWER-TMR is to be started or not; default is N.

The VM timeout is provisioned via the TYPE1=TO parameter in the Feature table (default 4 seconds).

- If Subscriber A has the default timer settings (that is, VM TO=4 seconds and NO-ANSWER-TIMER=185 seconds), and has the START-NO-ANSWER-TMR parameter set to Y (not the default), the call is processed as follows:

  [1] A calls B, B answers.

  [2] C calls A, A hears the CW tone, C hears ring tone.

  [3] If A does not attempt to answer the waiting call (C), and VM times out (4 seconds), C is forwarded according to normal VM forwarding procedures.

  However, if the VM timeout (TO) is set to a value *greater than* NO-ANSWER-TMR, when NO-ANSWER-TMR expires, C is disconnected and hears a busy tone, and VM is cancelled.

- If CHD is assigned to the subscriber along with CW, the following interaction occurs.
  - A (the subscriber) and B are on an active call.
  - C calls A.
  - A hears the CW tone. (C hears ringback.)
  - If A presses the **Flash** button or **hookswitch**, B is put on hold and A hears a dial tone.
  - If A dials *52, A is connected to C.
  - If A ignores the CW tone, C continues to hear ringback. The call is not forwarded.
- There is an interaction when a Centrex subscriber has all three of the following features assigned and active:
  1. Call hold—CHD.
  2. Call waiting—CW or CIDCW or both.
  3. Call forwarding on no answer—CFNA, VM (or VMA), or any combination of these.

  For information on this interaction, see the "CHD with CW/CIDCW and CFNA/VM/VMA" section on page 3-70.
- CW and DACWI Interaction for a CENTREX subscriber—If the DACWI feature is assigned to the called party (CENTREX subscriber), and the incoming call is from outside the CENTREX group, the called party is given a distinctive call-waiting indication. If the incoming call is from within the CENTREX group, the called party is *not* given a distinctive call-waiting indication, but a regular call-waiting indication is given.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the CW provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Cancel Call Waiting (CCW)

The Cisco BTS 10200 Softswitch supports cancel call waiting (CCW) feature activation as specified in LSSGR module FSD 01-02-1204 (TR-TSY-000572), *Cancel Call Waiting.*

CCW allows a user to disable CW, which also disables the CIDCW feature for the duration of a call (see the "Calling Identity Delivery on Call Waiting (CIDCW)" section on page 3-43). CCW is normally included as an integral part of a service package containing the CW and CIDCW features. CCW is useful when the user does not want to be interrupted during an important call or during an outgoing data/fax call.

The user activates and deactivates the CCW feature as follows:

- To make an uninterrupted new call:
  - The user lifts the handset, and listens for a dial tone.
  - The user enters the CCW VSC (for example, ***70**). The system responds by disabling the CW/CIDCW features and returning three short beeps and then the dial tone.
  - Now CCW is activated for the duration of the call, until the user goes on hook again.
  - After the user goes on hook, the CW/CIDCW service will be back in effect automatically.

Note There are exceptions. If a user was involved in a multiparty call, and received a ringback after going on hook, CCW remains active for the call.

- To make a currently active call go uninterrupted:
  - The user presses **Flash** button or **hookswitch**
  - The user enters the CCW VSC (for example, ***70**). The system responds by disabling the CW/CIDCW features and returning three short beeps and then the dial tone.
  - Now CCW is activated for the remainder of the current call, until the user goes on hook again.
  - The user presses **Flash** button or **hookswitch** to return to the original call.

After the current call is completely released, the CW service will be back in effect automatically.

Note If there is a CA switchover during an active call with CCW invoked, CCW will not be supported on that call after the switchover.

Tip To provision this feature, see the CCW provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Calling Identity Delivery on Call Waiting (CIDCW)

The BTS 10200 supports the calling identity delivery on call waiting (CIDCW) feature as specified in LSSGR module FSD 01-02-1090 (TR-TSY-000575), *Calling Identity Delivery on Call Waiting.*

CIDCW is a service that enables a called party to receive information about a calling party on a waiting call while off hook on an existing call. CIDCW provides the capability of calling identity delivery (CID) information to the called party on waiting calls. CIDCW is considered an enhancement of the CW feature, and requires the basic CW feature, along with the CND or CNAM feature.

Tip When CW and CIDCW are first provisioned by the service provider, they are active immediately by default. To assign these features in the deactivated state, configure the subscriber-feature-data table for that subscriber to make CW and CIDCW deactivated.

When a called party has been alerted of an incoming call, the called party places the current far-end party on hold by pressing the **Flash** button or **hookswitch** to retrieve the waiting call. The Flash button or hookswitch can be used to toggle between the current far-end party and the held party. The details of these functions are as follows:

- A called party currently on a call receives notification, via a short beep repeated 3 times, that another call is coming in.
- The incoming name and/or number is displayed after the first beep.
- The called party can either ignore the new call or can accept it while putting the existing call on hold.
- To ignore the new call, the called party continues uninterrupted on the existing call, and the beep indication will time out after 3 repetitions.
- To accept the new call and put the existing call on hold, the called party presses and releases the **Flash** button or **hookswitch**.
- To alternate between the two calls, the called party can press and release the **Flash** button or **hookswitch**.
- If either one of the remote stations goes on hook, the remaining remote station continues as a normal session with the called party.
- The called party can end either session by going on hook during the currently active session. This ends the session. The phone will ring to indicate that the other party is still holding. The called party can pick up the phone and the session to that calling party resumes as a normal call.

If the calling party's caller ID is not available (for example, if the caller has blocked caller ID) then the called party's caller ID display will indicate an anonymous call or other unidentified caller message as in the caller ID feature.

CIDCW Activation

CIDCW has multiple activation options as follows:

- Activated permanently at subscription time by service provider.

Tip When CW and CIDCW are first provisioned by the service provider, they are active immediately by default. To assign these features in the deactivated state, configure the subscriber-feature-data table for that subscriber to make CW and CIDCW deactivated.

- The feature can be activated by the individual user if the service provider has assigned the call waiting deluxe activation (CWDA) feature. The steps are as follows.
  - The user lifts the handset, and listens for a dial tone.
  - The user presses the activation VSC (for example, ***58**). If CIDCW can be activated, the system returns a success announcement. An error announcement, indicating the type of error, is given if activation is unsuccessful.

Note If CIDCW is already activated on this subscriber line, the activation attempt is accepted and processed as a new activation attempt.

- CIDCW is now activated, and will stay active until it is deactivated (see "CIDCW Deactivation" below).

CIDCW Deactivation

CIDCW deactivation options are as follows:

- Service provider deactivation at user request.
- The feature can be deactivated by the individual user if the service provider has assigned the call waiting deluxe deactivation (CWDD) feature. The steps are as follows.
  - The user lifts the handset and listens for a dial tone.
  - The user presses the deactivation VSC (for example, ***59**). A success announcement is given on a successful deactivation. An error announcement, indicating the type of error, is given if deactivation is unsuccessful.

Note If CIDCW is already deactivated on this subscriber line, the deactivation attempt is accepted and processed as a new deactivation attempt.

- CIDCW is now deactivated, and will stay inactive until it is activated (see "CIDCW Activation" above).

CIDCW Feature Interactions

- CW, CIDCW, and CWD interaction—CWD has a higher precedence than CIDCW, and CIDCW has a higher precedence than CW.
- There is an interaction when a Centrex subscriber has all three of the following features assigned and active:
  1. Call hold—CHD.
  2. Call waiting—CW or CIDCW or both.
  3. Call forwarding on no answer—CFNA, VM (or VMA), or any combination of these.

  For information on this interaction, see the "CHD with CW/CIDCW and CFNA/VM/VMA" section on page 3-70.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the CIDCW provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Call Waiting Deluxe (CWD)

CWD service informs a busy phone (user on an active call) that another call is waiting through the application of a call-waiting tone. Ten seconds after the initial tone, a second tone is applied if the waiting call has not been answered. To process the waiting call, the called party can take one of the following actions:

- The called party can go on hook to disconnect from the active call. The system will ring the called party, and the called party can take the phone off hook to be connected to the waiting call.
- To process the waiting call, the called party can press the **Flash** button or **hookswitch**. The system places the remote party on hold and provides a recall (stutter) dial tone to the called party. After receiving the recall dial tone, the called party can take one of the following actions:
  - If the called party presses digit **1**, the active call is dropped and a voice connection is established with the waiting party.
  - If the called party presses the digit **2**, a voice connection is established with the waiting party. From this point the called party can press the **Flash** button or **hookswitch**, receive recall dial tone, and press **2** to alternate between the parties.

While on a CWD call with the other two parties, the called party can exercise the following additional options after pressing the **Flash** button or **hookswitch** and receiving recall dial tone:

- If the called party presses digit **3** instead of 2, all three parties are conferenced together, and the call proceeds as in the three-way calling deluxe (TWCD) feature. (For more information on this call behavior, see the "Three-Way Calling Deluxe (TWCD)" section on page 3-122.)
- If the called party presses digit **1** instead of 2, the active call is dropped and a voice connection is established with the waiting party.
- If the called party goes on hook to disconnect from the active call, the system will ring the called party. The called party can take the phone off hook to be connected to the waiting call.

Note If a MGW-connected handset is off hook, but no active call exists (that is, receiving a dial tone), then an incoming call receives a busy tone and CWD is not activated.

Only one instance of CWD can be active for a given subscriber line at any given time. Thus, if a subscriber line were involved in both an active call and a waiting call, then an additional incoming call attempt results in the caller receiving a busy tone or being forwarded (CFB). The called party involved in the CWD call is not aware of the additional incoming call attempt.

The following conditions apply to the CWD feature:

- The CWD feature can be provided to POTS, Centrex, and MLHG subscribers.
- The CWD feature is in the deactivated mode unless activated by the subscriber.

The CWD feature is composed of four associated features, which are described in the sections that follow:

- CWD Activation, page 3-47
- CWD Deactivation, page 3-47
- CWD Interrogation, page 3-47
- CWD Invocation, page 3-48

CWD Timers

There are three timers that apply to the CWD feature:

- Call-waiting timeout timer (TO), measured in seconds—This is the time that an incoming call can be held in call-waiting mode. After the timer expires, the waiting call is disconnected. The default value is 15.
- Feature reconnect timer (FEATURE-RECONNECT-TMR), measured in seconds—During the course of using the CWD feature, if the subscriber is connected to a reorder tone or announcement, the subscriber is automatically reconnected to the previous call leg after the specified FEATURE-RECONNECT-TMR timeout period. The default value is 10.
- Reconnect timer (RECONNECT-TMR), measured in seconds—When a subscriber hangs up with another call on hold, the subscriber is rung back. The ringing is applied for the duration of this RECONNECT-TMR. If the subscriber does not answer the call within this time period, the call is torn down. The default value can be provisioned in the CA-CONFIG table. If the timer is not provisioned in the CA-CONFIG table, the preset value 36 is used as default.

CWD Activation

CWD has multiple activation options as follows:

- Activated permanently at subscription time by service provider.
- Activated by user:
  - The user lifts the handset, and listens for a dial tone.
  - The user presses the activation VSC (for example, ***58** in North America and ***58#** in China). If CWD can be activated, the system returns a success announcement. An error announcement, indicating the type of error, is given if activation is unsuccessful.
  - CWD is now activated, and will stay active until it is deactivated (see "CWD Deactivation" below).

CWD Deactivation

CWD 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, ***59** in North America and **#58#** in China). A success announcement is given on a successful deactivation. An error announcement, indicating the type of error, is given if deactivation is unsuccessful.
  - CWD is now deactivated, and will stay inactive until it is activated (see "CWD Activation" above).

CWD Interrogation

CWD interrogation allows a user to check whether CWD is activated on his or her local phone. The user enters the VSC for CWD interrogation (for example, ***56** in North America and ***#58#*** in China). A success announcement is given to the user if CWD is activated, and an appropriate announcement is provided if it is deactivated.

CWD Invocation

CWD invocation is the actual set of procedures the system follows when a user (with CWD activated) is already on an active call and receives a call from a third party.

Invalid User Actions

The valid user actions are described in the sections above. The following user actions are invalid, and the system provides an appropriate error announcement:

- The user tries to interrogate CWD on a fresh system (a system with no entry in the SUBSCRIBER-FEATURE-DATA table).
- The user presses the Flash button or hookswitch, receives recall dial tone, and then enters a digit other than 1, 2, or 3.

CWD Feature Interactions

CWD and CFNA Interaction—If both CFNA and CWD are subscribed to and activated by the user, the interaction is as follows. If the user is on an active call when a new call comes in, the CWD tone will be played. The CWD feature does not perform any timing in this case (that is, CWD does not start the call-waiting disconnect timer). If the user presses the hookswitch before the CFNA timer runs out, the user will be connected to the new call, and the call will proceed according to the CWD feature. If the user takes no action, and the CFNA timer runs out, the waiting call will be forwarded per the CFNA procedure.

CWD and CFB Interaction—If both CWD and CFB are activated, CWD has higher precedence than CFB.

CWD and TWCD Interaction—These two feature invocations are mutually exclusive. When one feature is invoked, the other feature is not allowed.

Note During a three-way call, the CWD feature does not work for the party that initiated the three-way call. However, the CWD feature would work normally for the other two (non-initiating) parties.

CWD and CLIP interaction—If the called user is given a call waiting indication, and has subscribed to the CLIP service, then the calling line identification is presented to the user at the time the call waiting indication is given.

CWD, CIDCW, CW Interaction—CWD has a higher precedence than CIDCW, and CIDCW has a higher precedence than CW.

CWD and CCW Interaction—When CCW is activated, CWD will be inhibited. (Note that CCW is a per-call activated feature.)

CWD and DRCW Interaction—If the calling party number is in the DRCW list of the called party, and if DRCW is activated, the called party is given a distinctive call-waiting indication. Otherwise, the regular call-waiting indication is given.

CWD and DACWI Interaction for a CENTREX subscriber—If the DACWI feature is assigned to the called party (CENTREX subscriber), and the incoming call is from outside the CENTREX group, the called party is given a distinctive call-waiting indication. Otherwise, the regular call-waiting indication is given.

CWD and MDN Interaction—If the calling party dials the called party number different from main number, the called party is given a distinctive call-waiting indication. Otherwise, the regular call waiting indication is given.

CWD and DACWI Interaction—If this is a direct inward dialing (DID) call and DACWI feature is assigned, the called party is given a distinctive call-waiting indication. Otherwise, a regular call-waiting indication is given.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the CWD provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Calling Identity Features

Calling identity features include:

- Calling Identity Delivery, page 3-49
  - Calling Number Delivery (CND), page 3-50
  - Calling Name Delivery (CNAM), page 3-50
- Calling Line Identification Presentation (CLIP), page 3-50
- Calling Identity Delivery Blocking (CIDB), page 3-52
  - Calling Number Delivery Blocking (CNDB), page 3-53
  - Calling Name Delivery Blocking (CNAB), page 3-53
  - Calling Identity Delivery and Suppression (CIDSD and CIDSS), page 3-54
- Calling Line Identification Restriction (CLIR), page 3-55
  - Calling Number Delivery Blocking (CNDB), page 3-56
  - Calling Name Delivery Blocking (CNAB), page 3-57
  - Calling Identity Delivery and Suppression (CIDSD and CIDSS), page 3-57

Note The calling identity delivery on call waiting (CIDCW) feature is described in the "Call Waiting Features" section on page 3-39.

Calling Identity Delivery

The identity of the caller is provided in two features, calling number delivery (CND) and calling name delivery (CNAM), as described in the following sections.

Calling Number Delivery (CND)

The BTS 10200 supports the CND feature as specified in the Telcordia LSSGR module FSD 01-02-1051 (TR-NWT-000031), *Calling Number Delivery, and GR-30-CORE, Voiceband Data Transmission Interface.*

The CND feature provides CPE with the date, time, and DN of an incoming call. When the called subscriber line is on hook, the calling party information is delivered during the long silent interval of the first ringing cycle. Telcordia document GR-30-CORE specifies the generic requirements for transmitting asynchronous voice band data to the CPE.

Tip To provision this feature, see the CND provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Calling Name Delivery (CNAM)

The BTS 10200 supports the CNAM feature as specified in LSSGR module FSD 01-02-1070 (TR-TSY-001188), *Calling Name Delivery Generic Requirements.*

CNAM is a terminating user feature allowing CPE connected to a switching system to receive a calling party's name, number, and the date and time of the call during the first silent interval. If a private status is assigned with the name, the name will not be delivered and a private indicator code P is sent to the CPE. If the name is not available for delivery, the switch sends an out-of-area/unavailable code O to the CPE. When transferring or forwarding calls internally, the private calling name can be obtained from the Cisco BTS 10200 Softswitch databases and passed on to the internal called user.

Tip To provision this feature, see the CNAM provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Calling Line Identification Presentation (CLIP)

This section describes the calling line identification presentation (CLIP) feature. This feature is available to POTS, Centrex, and MLHG subscribers.

References:

- Telcordia LSSGR, *CLASS Feature: Calling Number Delivery, GR-31-CORE*
- ITU-T: I.251.3 (08/92) *Calling Line Identification Presentation*

CLIP Feature Description

CLIP is a supplementary service offered to the called party that displays the calling party DN and the date and time of the call. The calling line identification information is included in the incoming message (for example, SETUP, IAM, R2 digits, SIP, and so forth) from the originating DN. Interoffice application of this service depends on network deployment of signaling methods capable of transmitting the calling line identification.

The Cisco BTS 10200 Softswitch supports this feature for the following types of incoming calls:

- Intraoffice calls—Calls that originate and terminate on lines supported by one Cisco BTS 10200 Softswitch. (The calling party's DN is retrieved from the Cisco BTS 10200 Softswitch memory.)
- Incoming interoffice calls from another Cisco BTS 10200 Softswitch on the packet network.
- Incoming interoffice calls from another stored program controlled switch (SPCS) on the packet network or the connection-oriented network.

The calling party's information can be public, private, or unavailable:

- Public—If the calling line identification information is included in the message from the originating DN, and is not blocked, the Cisco BTS 10200 Softswitch displays it on the called party's display.
- Private (anonymous)—If the calling line DN has been marked to indicate that it is private, the Cisco BTS 10200 Softswitch does not transmit the DN to the called party. Instead, it sends the date, time, and a private indicator, signified by the ASCII letter "P", to the called party in place of the calling line DN.
- Unavailable—If the calling line identification information is not available, the Cisco BTS 10200 Softswitch displays an out-of-area/DN-unavailable indicator, signified by the ASCII letter "O", along with the date and time.

CLIP Feature Activation and Deactivation

CLIP is offered to users on a subscription basis. Once the feature has been successfully assigned, the called party should receive the date, time, and calling number, if available and allowed to be disclosed, for all subsequent incoming calls. If the called party does not subscribe to this feature, the calling party's identity information is not transmitted to the called party's handset.

CLIP Feature Interactions

CFU—When CLIP is subscribed and the user activates CFU, all incoming calls are forwarded at the base phone, and the Cisco BTS 10200 Softswitch forwards the original calling DN to the remote phone.

CFNA—When CLIP is subscribed and the user activates CFNA, all unanswered incoming calls are forwarded at the base phone, and the Cisco BTS 10200 Softswitch forwards the original calling DN to the remote phone.

CFB—When CLIP is subscribed and the user activates CFB, incoming calls are forwarded when the base phone is off hook, and the Cisco BTS 10200 Softswitch forwards the original calling DN to the remote phone.

CLIR—There are no interactions between CLIP and CLIR when active on the same line. Indirect interactions occur between CLIP and CLIR when the calling party subscribes to CLIR and the called party subscribes to CLIP. If the calling party uses any of the CLIR features to make the status of the calling DN private, the terminating SPCS (Cisco BTS 10200 Softswitch) transmits a "P" (indicating private status) to the terminating phone.

CWD—If the called user is given a call waiting indication, and has subscribed to the CLIP service, then the calling line identification is presented to the user at the time the call waiting indication is given.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the CLIP provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Calling Identity Delivery Blocking (CIDB)

The Cisco BTS 10200 Softswitch supports calling identity delivery blocking (CIDB) features as specified in LSSGR module FSD 01-02-1053 (TR-NWT-000391), *Calling Identity Delivery Blocking Features*

CIDB allows caller to control whether or not their calling identity information is delivered with outgoing calls. Identity includes directory number (DN) and/or name of the caller. CIDB does not affect the presentation of caller's information when making 911 calls.

The CIDB feature affects the presentation status (PS) of the calling identity information. The PS is a flag that lets the network know if it is permissible to deliver the information to the called party. Both the calling number and calling name have PS information associated with them. There are two types of PS flags—permanent and per-call:

- Permanent PS (PPS)—The service provider provisions PPS flags, either public or private, for each subscriber line. These values are defined as follows:
  - Public—Calling identity information (calling name and/or calling number) is delivered with outgoing calls. The local switch (BTS 10200) informs the remote switch that it is permissible to deliver the caller's identity information on the remote phone.
  - Private (anonymous)—Calling identity information (calling name and/or calling number) is not delivered with outgoing calls. The local switch (BTS 10200) informs the remote switch that it is **not** permissible to deliver the caller's identity information on the remote phone.
- Per-call PS (PCPS) has significance only to the current outgoing call. On a per-call basis, a caller with the CIDB feature enabled can override the default values for the PS flags. The per-call features are listed in Table 3-7 and described in the "Calling Number Delivery Blocking (CNDB)" section on page 3-53 through the "Calling Identity Delivery and Suppression (CIDSD and CIDSS)" section on page 3-54.

Note The vertical service codes (VSCs), also called star codes, listed in Table 3-7 and throughout this section are typical values. The service provider can provision these values with any valid unique ASCII string up to five characters long. For a complete list of valid VSC formats and preprovisioned VSCs, see the VSC table specification and VSC appendix in the *Cisco BTS 10200 Softswitch CLI Reference Guide*.

Table 3-7 Per-Call CIDB Feature Summary

Identity Item	Permanent Privacy Status (PPS)		Effect Of CNDB (*67)		Effect Of CNAB (*95)		Effect Of CIDSD (*82)		Effect Of CIDSS (*96)	
	Number	Name	Number PS	Name PS	Number PS	Name PS	Number PS	Name PS	Number PS	Name PS
Identity:	Public	Public	Private	Private[1]	Public	Private	Public	Public	Private	Private
Number [CND]	Public	Private	Private	Private	Public	Public	Public	Public	Private	Private
	Private	Public[1]	Public	Public	Private	Private	Public	Public	Private	Private
+ Name [CNAM]	Private	Private	Public	Private	Private	Private[1]	Public	Public	Private	Private
Number:	Public	n/a	Private	n/a	n/a	n/a	Public	n/a	Private	n/a
[CND] only	Private	n/a	Public	n/a	n/a	n/a	Public	n/a	Private	n/a

1. When the number is private, no name query is performed.

When a caller goes off hook and does not enter a per-call CIDB code that affect the caller's PS, then the value of the caller's PPS is used as the presentation status for that call. When a CIDB per-call feature is used on a call, only the current call is affected. The PPS is used for future calls (unless the caller enters one of the per-call features again.)

Calling Number Delivery Blocking (CNDB)

Calling number delivery blocking (CNDB) allows the caller to control the status of their caller number privacy on a per-call basis. For all new calls, the privacy status reverts back to the PPS.

To use the CNDB feature, the caller does the following:

- The caller goes off hook and receives a dial tone.
- The caller enters the CNDB VSC (for example, ***67**). The system responds with a dial tone.
- The caller enters the desired phone number for the remote station. The CNDB function toggles the PPS of the caller's number for this call:
  - If the PPS is private, CNDB makes the PS public for this call
  - If the PPS is public, CNDB makes the PS private for this call

Note When the number is private, no name query is performed.

Tip To provision this feature, see the CNDB provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Calling Name Delivery Blocking (CNAB)

Calling name delivery blocking (CNAB) allows the caller to control the status of their caller name privacy on a per-call basis. For all new calls, the privacy status reverts back to the PPS.

To use the CNAB feature, the caller does the following:

- The caller goes off hook and receives a dial tone.
- The caller enters the CNAB VSC (for example, ***95**). The system responds with a dial tone.
- The caller enters the desired phone number for the remote station. The CNAB function toggles the PPS of the caller's name for this call:
  - If the PPS is private, CNAB makes the PS public for this call
  - If the PPS is public, CNAB makes the PS private for this call

Note When the number is private, no name query is performed.

Note The CNAB feature is not supported over SIP trunks.

Tip To provision this feature, see the CNAB provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Calling Identity Delivery and Suppression (CIDSD and CIDSS)

The BTS 10200 supports the delivery function and the suppression function of calling identity delivery and suppression (CIDSD and CIDSS, respectively). CIDSD and CIDSS are per-call features.

CIDSD and CIDSS allow a caller to explicitly indicate on a per-call basis whether both the calling name and calling number will be treated as private or public. When CIDSD or CIDSS is used, the system does not query the PPS of the caller's DN and name. The following conditions apply:

- CIDS Delivery (CIDSD)—If the caller enters the VSC for CIDSD (for example, ***82**), the current call is treated as public regardless of the default privacy status permanently associated with the calling name and number.
- CIDS Suppression (CIDSS)—If the caller enters the VSC for CIDSS (for example, ***96**), the current call is treated as private regardless of the default privacy status permanently associated with the calling name and number.

For all new calls, the privacy status reverts back to the PPS.

To use the CIDSD or CIDSS feature, the caller does the following:

- The caller goes off hook and receives a dial tone.
- The caller enters the VSC for CIDSD or CIDSS (for example, ***82** or ***96**) and receives a dial tone again.
- The caller enters the desired phone number for the remote phone.
- The caller's ID will be displayed or blocked as follows:
  - For *82, the caller's ID will be delivered (that is, it will not be blocked) at the remote station, assuming the remote station has the caller ID function.
  - For *96, the caller's ID will be blocked at the remote station, assuming the remote station has the caller ID function.

The next time this caller makes a phone call, the default caller ID settings (PPS) will apply, unless the caller again enters the VSC for CIDSD or CIDSS.

Tip To provision these features, see the CIDSD and CIDSS provisioning procedures in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Calling Line Identification Restriction (CLIR)

This section describes the calling line identification restriction (CLIR) feature. This feature is available to POTS, Centrex, and MLHG subscribers.

References:

- Telcordia LSSGR, *CLASS Feature: Calling Identity Delivery Blocking Features, GR-391-CORE*
- ITU-T: I.251.4 (08/92) *Calling Line Identification Restriction*

CLIR is a supplementary service that allows callers to control whether or not their calling identity information is delivered with outgoing calls. Identity includes directory number (DN) and/or name of the caller. The presentation of calling identity information (at the terminating phone) is described in the "Calling Line Identification Presentation (CLIP)" section on page 3-50.

When provisioned by the service provider, the calling party can restrict the display of his or her DN on either a permanent basis or a per-call basis. The CLIR feature consists of the following per-call associated features:

- Calling Number Delivery Blocking (CNDB), page 3-56
- Calling Name Delivery Blocking (CNAB), page 3-57
- Calling Identity Delivery and Suppression (CIDSD and CIDSS), page 3-57

Calling Identity Presentation Status

The CLIR feature affects the presentation status (PS) of the calling identity information. The PS is a flag that lets the network know if it is permissible to deliver the information to the called party. Both the calling number and calling name have PS information associated with them. There are two types of PS flags—permanent and per-call:

- Permanent PS (PPS)—The service provider provisions PPS flags, either public or private, for each subscriber line. These values are defined as follows:
  - Public—Calling identity information (calling name and/or calling number) is delivered with outgoing calls. The local SPCS (Cisco BTS 10200 Softswitch) informs the remote SPCS that it is permissible to deliver the caller's identity information to the remote phone.
  - Private (anonymous)—Calling identity information (calling name and/or calling number) is not delivered with outgoing calls. The local SPCS (Cisco BTS 10200 Softswitch) informs the remote SPCS that it is *not* permissible to deliver the caller's identity information to the remote phone.
- Per-call PS (PCPS) has significance only to the current outgoing call. On a per-call basis, a caller with the CLIR feature enabled can override the default values for the PS flags. The per-call features are listed in Table 3-8 and described in the "Calling Number Delivery Blocking (CNDB)" section on page 3-56 through the "Calling Identity Delivery and Suppression (CIDSD and CIDSS)" section on page 3-57.

Note The vertical service codes (VSCs), also called star codes, listed in Table 3-8 and throughout this section are typical values. The service provider can provision these values with any valid unique ASCII string up to five characters long. For a complete list of valid VSC formats and preprovisioned VSCs, see the VSC table specification and VSC appendix in the *Cisco BTS 10200 Softswitch CLI Reference Guide*.

Table 3-8 Per-Call CLIR Feature Summary

Identity Item	Permanent Privacy Status (PPS)		Effect Of CNDB (*67*)		Effect Of CNAB (*95*)		Effect Of CIDSD (*82*)		Effect Of CIDSS (*96*)	
	Number	Name	Number PS	Name PS	Number PS	Name PS	Number PS	Name PS	Number PS	Name PS
Identity:	Public	Public	Private	Private[1]	Public	Private	Public	Public	Private	Private
Number [CND]	Public	Private	Private	Private	Public	Public	Public	Public	Private	Private
	Private	Public[1]	Public	Public	Private	Private	Public	Public	Private	Private
+ Name [CNAM]	Private	Private	Public	Private	Private	Private[1]	Public	Public	Private	Private
Number:	Public	n/a	Private	n/a	n/a	n/a	Public	n/a	Private	n/a
[CND] only	Private	n/a	Public	n/a	n/a	n/a	Public	n/a	Private	n/a

1. When the number is private, no name query is performed.

When a caller goes off hook and does not enter a per-call CLIR code that affect the caller's PS, then the value of the caller's PPS is used as the presentation status for that call. When a CLIR per-call feature is used on a call, only the current call is affected. The PPS is used for future calls (unless the caller enters one of the per-call features again.)

Calling Number Delivery Blocking (CNDB)

The CNDB associated feature affects the PS designation of the caller's DN. CNDB works as follows:

- The caller goes off hook and receives dial tone.
- The caller enters the CNDB VSC (for example, ***67***). The system responds with a dial tone.
- The caller enters the desired phone number for the remote phone. The local switch (Cisco BTS 10200 Softswitch) retrieves the PPS value of the DN for the caller's line, and then forwards the *opposite of the PS value* to the remote switch. Therefore:
  - If the PPS of the DN is public, the Cisco BTS 10200 Softswitch sends a PCPS of private.
  - If the PPS of the DN is private, the Cisco BTS 10200 Softswitch sends a PCPS of public.

Note When the number is private, no name query is performed.

Tip To provision this feature, see the CNDB provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Calling Name Delivery Blocking (CNAB)

The CNAB associated feature affects the PS designation of the caller's name. CNAB works as follows:

- The caller goes off hook and receives dial tone.
- The caller enters the CNAB VSC (for example, ***95***). The system responds with a dial tone.
- The caller enters the desired phone number for the remote phone. The local switch (Cisco BTS 10200 Softswitch) retrieves the PPS value of the name for the caller's line, and then forwards the *opposite of the PS value* to the remote switch. Therefore:
  - If the PPS of the name is public, the Cisco BTS 10200 Softswitch sends a PCPS of private.
  - If the PPS of the name is private, the Cisco BTS 10200 Softswitch sends a PCPS of public.

Note When the number is private, no name query is performed.

Note The CNAB feature is not supported over SIP trunks.

Tip To provision this feature, see the CNAB provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Calling Identity Delivery and Suppression (CIDSD and CIDSS)

The BTS 10200 supports the delivery function and the suppression function of calling identity delivery and suppression (CIDSD and CIDSS, respectively). CIDSD and CIDSS are per-call features.

CIDSD and CIDSS allow a caller to explicitly indicate on a per-call basis whether both the calling name and calling number will be treated as private or public. When CIDSD or CIDSS is used, the system does not query the PPS of the caller's DN and name. The following conditions apply:

- CIDS Delivery (CIDSD)—If the caller enters the VSC for CIDSD (for example, ***82***), the current call is treated as public regardless of the default privacy status permanently associated with the calling name and number.
- CIDS Suppression (CIDSS)—If the caller enters the VSC for CIDSS (for example, ***96***), the current call is treated as private regardless of the default privacy status permanently associated with the calling name and number.

For all new calls, the privacy status reverts back to the PPS.

To use the CIDSD or CIDSS feature, the caller does the following:

- The caller goes off hook and receives a dial tone.
- The caller enters the VSC for CIDSD or CIDSS (for example, ***82*** or ****96***) and receives a dial tone again.
- The caller enters the desired phone number. for the remote phone
- The caller's ID will be displayed or blocked as follows:
  - For *82*, the caller's ID will be delivered (that is, it will not be blocked) at the remote station, assuming the remote station has the caller ID function.

– For *96*, the caller's ID will be blocked at the remote station, assuming the remote station has the caller ID function.

The next time this caller makes a phone call, the default caller ID settings (PPS) will apply, unless the caller again enters the VSC for CIDSD or CIDSS.

Tip To provision these features, see the CIDSD and CIDSS provisioning procedures in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

CLIR Feature Interactions

CLIP—There are no interactions between CLIP and CLIR when active on the same line. Interactions occur between CLIP and CLIR when the calling party subscribes CLIR and the called party subscribes to CLIP. If the calling party uses any of the CLIR features to make the status of the calling DN private, the terminating SPCS (Cisco BTS 10200 Softswitch) transmits a "P" (indicating private status) to the terminating phone.

TWCD—A user with TWCD can press the Flash button or hookswitch and use any of the CLIR per-call restrictions before dialing the next phone number. This allows the user to control the presentation of his or her PS to the third party in the three-way call.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the CLIR provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Direct Inward/Outward Dialing for PBX

The Cisco BTS 10200 Softswitch supports the direct inward dialing (DID) and direct outward dialing (DOD) features for PBX.

Analog DID for PBX

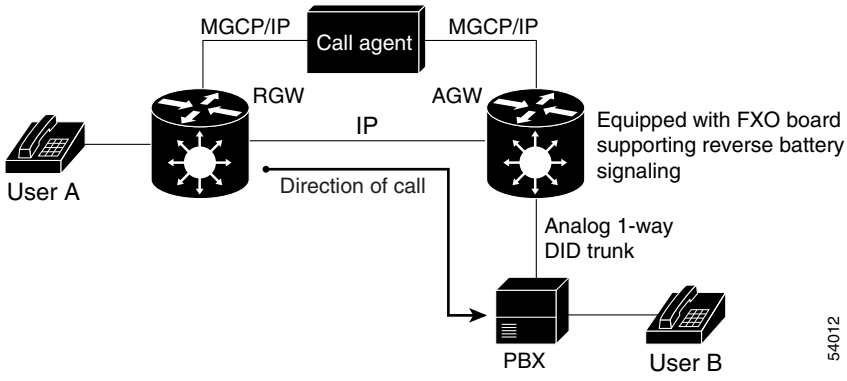
The Cisco BTS 10200 Softswitch supports analog DID for PBX as specified in TIA/EIA-464B, *Requirements for Private Branch Exchange (PBX) Switching Equipment*, April 1, 1996.

The analog DID one-way feature allows incoming calls to a local PBX network to complete to a specific station without attendant assistance. The station address is provided by the CA that controls an access gateway (AGW) connecting to the PBX. The number of digits to be outpulsed by the AGW to the PBX is configurable in the CA.

Note For guidance in provisioning the CA to support this feature, see the Cisco *BTS 10200 Softswitch Operations Manual.*

Figure 3-1 shows a typical application, with a residential user (UserA) attempting to call a PBX user station (UserB). UserB is identified by a specific set of extension digits in the PBX. The Cisco BTS 10200 Softswitch uses MGCP signaling to communicate with the AGW, and controls the outpulsing of digits from the AGW to the PBX. A foreign exchange office (FXO) board in the AGW uses reverse battery signaling (per TIA/EIA-464B) to communicate with a DID trunk board in the PBX over an analog DID one-way trunk. When completing a call termination to the PBX, the extension digits for UserB are outpulsed from the AGW toward the PBX. The PBX receives the extension digits and then completes the call to UserB.

Figure 3-1 Example of PBX Analog DID One-Way Application



Tip To provision PBX-DID subscribers, you must use the proper settings in the DN to Subscriber (dn2subscriber) and Subscriber (subscriber) tables. See the IAD Subscriber provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

DOD For PBX

Reference: LSSGR module FSD 04-02-0000 (TR-TSY-000524), *Direct Inward Dialing*.

The DOD feature allows outgoing calls from a specific station to be completed through the local PBX network without attendant assistance. The CA serving the PBX recognizes the station address and routes the call to the PBX.

Seasonal Suspend

The Seasonal Suspend feature is available in Release 5.0, MR1. In Release 5.0, MR1.1, changes were made to enhance the usability of this feature. (MR1,1 simplifies the steps for putting a subscriber in seasonal suspend status.) This document is divided into separate parts for the two maintenance releases. Make sure that you use the section that applies to the release (MR1 and earlier, or MR1.1 and later) you are running on your system:

- "Seasonal Suspend Feature for Release 5.0 MR1 and Earlier" section on page 3-60
- "Seasonal Suspend Feature for Release 5.0 MR1.1 and Later" section on page 3-63

This document includes references to specific CLI database tables and parameters. For a complete listing of all tables and parameters, see the *Cisco BTS 10200 Softswitch CLI Database*.

Seasonal Suspend Feature for Release 5.0 MR1 and Earlier

Use this section if your system is running Release 5.0, MR1 or earlier.

Understanding the Seasonal Suspend Feature, MR1 and Earlier

The Seasonal Suspend feature allows subscribers to suspend their telephone service (instead of disconnecting it) while they are away for the off-season. This feature affects both inbound and outbound calls on the subscriber line.

Note In this document, "inbound calls" means calls that are intended to be terminated on the seasonal suspend subscriber line. "Outbound calls" means calls that are originated by a user on the seasonal suspend line.

Allowed and Disabled Features for Outbound Calls

During the suspension period, outbound calls are treated as follows:

- Allowed features—Emergency (911), toll-free customer service numbers such as repair (611), and voice mail. The subscriber can retrieve messages and access voice-mail functions by dialing the voice-mail pilot number.
- Disabled features—All domestic and international inbound and outbound calling, operator services, directory assistance, caller ID blocking, vertical service codes (VSCs), midcall and hookflash-based features, and all calling features other than the allowed features listed above.

Treatment of Outbound Calls

You can provision the system (through the feature-configuration table) to provide special handling for outbound calls that are blocked by seasonal suspend. You can provide either of the following treatments:

- Route outbound calls to a standard announcement indicating that seasonal suspend is active on the subscriber line. This is the default behavior.
- Route outbound calls to a customer support line. (You provision the support line directory number [DN] in the feature-configuration table.)

Treatment of Inbound Calls

The system provides special handling for inbound calls that are rejected due to seasonal suspend status. You can provide either of the following treatments:

- Play a generic seasonal suspend announcement. This is the default behavior.
- Play a seasonal suspend announcement that includes a DN at which the subscriber can be reached. This DN is provisionable in the subscriber-feature-data table.

If the Voice Mail Always (VMA) feature is provisioned and active on the subscriber line prior to the time you set the subscriber status to seasonal suspend, VMA continues to function during the seasonal suspend period and takes precedence over Seasonal Suspend features for inbound calls.

Deactivation of Seasonal Suspend

At the request of the subscriber, the service provider deactivates the Seasonal Suspend feature by resetting two parameters in the Subscriber table:

- Set status=active.

- Set cos-restrict-id to the same value it had prior to the start of seasonal suspend.

Note You can set the subscriber status to active, or to any other valid status other than seasonal-suspend, by provisioning the status parameter in the Subscriber table.

Feature Interactions

This section describes interactions of this feature with other telephony features.

- VMA for inbound calls to the subscriber line—By design, VMA (if provisioned, activated, and available) takes precedence over any inbound call routing for seasonal suspend. In this case, the system provides VMA to all inbound calls, and not seasonal suspend.
- Other calling features—If you assign seasonal suspend status to a subscriber, the system does not provide any other features for this subscriber except those listed below. You must provision these options through a special Class of Service (CoS) restriction.
  - Calls allowed in the seasonal suspend cos-restrict table, which can include repair, a customer service number, and a voice-mail pilot number if provisioned
  - Calls provisioned with the trigger-nod-escape-list command

The subscriber line can be used to make calls to a limited number of DNs, such as emergency services, customer service or repair service, voice-mail pilot number, or to other DNs allowed in the national-wb-list. During such a call, if an operator attempts to perform Busy Line Verification (BLV), the call from the operator receives the same treatment as that provisioned for any other incoming call to this subscriber, that is, forwarding to VMA or forwarding to a seasonal suspend announcement.

- Billing treatment—The system generates the following billing cause codes for this feature:
  - Outbound calls that are blocked due to seasonal suspend result in billing cause code SERVICE_DENIED. Outbound calls that are redirected to the customer service number result in normal billing record events.
  - Inbound calls that are blocked or redirected due to seasonal suspend result in the billing cause code CALL_REJECTED.

Prerequisites

This section lists requirements that must be met before the feature can work.

Announcements

The appropriate announcements must be provisioned and available on the system, including announcements for generic seasonal suspend and DN referral. See release cause codes 1272 through 1275 and the associated announcements in the "Cause Code to Announcement ID Mappings" section of the *Cisco BTS 10200 Softswitch Provisioning Guide*. Routing to the announcement server must be working properly.

Note For features requiring an audible DN readout, such as seasonal suspend, the BTS 10200 has been tested for interoperability with the ThinkEngine Networks announcement server, Models 500X and 4000X.

VMA Treatment of Inbound Calls

This prerequisite applies if you are provisioning a customer with VMA treatment (instead of seasonal suspend treatment) for inbound calls.

The subscriber must have VMA activated and provisioned through the interactive voice response (IVR) provisioning system before you set the subscriber status to seasonal-suspend. If VMA is assigned and active, inbound calls to this subscriber are given VMA treatment instead of seasonal suspend treatment. However, outbound calls receive seasonal-suspend treatment if status=seasonal-suspend.

Caution VMA, if assigned and active, takes precedence over the Seasonal Suspend feature. In this case, incoming calls *do not* receive seasonal suspend treatment. The incoming calls go directly to voice mail, and *not* to a seasonal suspend message, even if a seasonal suspend message is provisioned. Therefore, if the end user wishes to have seasonal suspend treatment for inbound calls, make sure that VMA is *deactivated* before setting status=seasonal-suspend.

Limitations

This section lists limitations for the Seasonal Suspend feature. These are conditions for which the Seasonal Suspend feature is not designed to work or works in a limited manner.

- This feature is not available to Centrex or multiline hunt group (MLHG) subscribers.
- The BTS 10200 does not support start and end timing for this feature.

Restrictions

This section lists restrictions. These are conditions that might cause this feature to fail or work improperly.

VMA Option

VMA, if provisioned and active, takes precedence over the Seasonal Suspend feature for treatment of inbound calls. The customer can call the VMA access DN (voice-mail pilot number) from any phone to use the voice-mail system. However, the following restrictions apply to calls placed from the seasonal subscriber line to the voice-mail pilot number:

- The customer can reach the voice-mail pilot number from the seasonal suspend phone only by calling the pilot number directly. The customer cannot use a vertical service code (VSC) for this purpose, because VSCs do not work on a seasonal suspend line.
- If you want the customer to be able to dial the voice-mail pilot number, you must provision this pilot DN for white list treatment in the national-wb-list table and link this DN to the seasonal suspend cos-restrict table. See the applicable steps in the “Office Provisioning” section of “Seasonal Suspend Provisioning for MR1 and Earlier” section in *Cisco BTS 10200 Softswitch Provisioning Guide*.

DN Readout by Announcement Server

Cisco has tested the ability of certain announcement servers to interwork with the BTS 10200 to provide DN-readout announcements. See the “Component Interoperability” section of the *Cisco BTS 10200 Softswitch Release Notes* for information on the capable announcement servers. Other announcement servers might also work, but might not have been tested for interoperability by Cisco.

Restoring COS Restrictions

When you provision a subscriber for seasonal suspend, you must create a special CoS restriction and assign it to the subscriber. This CoS restriction (cos-restrict-id in the Subscriber table) replaces the cos-restriction-id value that was originally assigned to this subscriber. The system does not track the original setting. Therefore, you must have a method of retaining a record of the original cos-restrict-id for each subscriber so you can restore it at the end of the seasonal suspend period.

Provisioning

Refer to the "Seasonal Suspend Provisioning for MR1 and Earlier" section in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Seasonal Suspend Feature for Release 5.0 MR1.1 and Later

Use this section if your system is running Release 5.0, MR1.1 or later.

Understanding the Seasonal Suspend Feature, MR1.1 and Later

The Seasonal Suspend feature allows subscribers to suspend their telephone service (instead of disconnecting it) while they are away for the off-season. This feature affects both inbound and outbound calls on the subscriber line.

Note In this document, inbound calls means calls that are intended to be terminated on the seasonal suspend subscriber line. Outbound calls means calls that are originated by a user on the seasonal suspend line.

Allowed and Disabled Features for Outbound Calls

During the suspension period, outbound calls are treated as follows. (The exact treatment depends on several provisioned values as described in this document.)

- Allowed features—Emergency (911), toll-free customer service numbers such as repair (611), and voice mail. The subscriber can retrieve messages and access voice-mail functions by dialing the voice-mail pilot number.
- Disabled features—All domestic and international inbound and outbound calling, operator services, directory assistance, caller ID blocking, vertical service codes (VSCs), midcall and hookflash-based features, and all calling features other than the allowed features listed above.

Treatment of Outbound Calls

You can provision the system (through the feature-configuration table) to provide special handling for outbound calls that are blocked by seasonal suspend. You can provide either of the following treatments:

- Route outbound calls to a standard announcement indicating that seasonal suspend is active on the subscriber line. This is the default behavior.
- Route outbound calls to a customer support line. (You provision the support line directory number [DN] in the feature-configuration table.)

Treatment of Inbound Calls

The system provides special handling for inbound calls that are rejected due to seasonal suspend status. You can provide either of the following treatments:

- Play a generic seasonal suspend announcement. This is the default behavior.
- Play a seasonal suspend announcement that includes a DN at which the subscriber can be reached. This DN is provisionable in the subscriber-feature-data table.

If the Voice Mail Always (VMA) feature is provisioned and active on the subscriber line prior to the time you set the subscriber status to seasonal suspend, VMA continues to function during the seasonal suspend period, and takes precedence over Seasonal Suspend features for inbound calls.

Deactivation of Seasonal Suspend

At the request of the subscriber, you can deactivate the Seasonal Suspend feature by setting status=active (or any status other than seasonal-suspend).

Note You can set the subscriber status to active, or to any other valid status other than seasonal-suspend, by provisioning the status parameter in the Subscriber table.

Feature Interactions

This section describes interactions of this feature with other telephony features.

- VMA for inbound calls to the subscriber line—By design, VMA (if provisioned, activated, and available) takes precedence over any inbound call routing for seasonal suspend. In this case, the system provides VMA to all inbound calls, and not seasonal suspend.
- Other calling features—If you assign seasonal suspend status to a subscriber, the system does not provide any other features for this subscriber except those listed below. You must provision these options through a special class of service (CoS) restriction for seasonal suspend. When you set the subscriber status to seasonal-suspend, the system automatically uses this system-wide seasonal suspend CoS restriction, and *not* the CoS restriction that is assigned individually to the subscriber. As described in the "Seasonal Suspend Provisioning MR1.1 and Later" section in the *Cisco BTS 10200 Softswitch Provisioning Guide* you can allow the following types of calls for subscribers in seasonal suspend status:
  - Calls with call type EMG (emergency calls)
  - Calls allowed in the seasonal suspend cos-restrict table, which can include repair, a customer service number, and a voice-mail pilot number if provisioned
  - Calls provisioned with the trigger-nod-escape-list command

The subscriber line can be used to make calls to a limited number of DNs, such as emergency services, customer service or repair service, voice-mail pilot number, or to other DNs allowed in the national-wb-list. During such a call, if an operator attempts to perform Busy Line Verification (BLV), the call from the operator receives the same treatment as that provisioned for any other incoming call to this subscriber, that is, forwarding to VMA or forwarding to a seasonal suspend announcement.

- Billing treatment—The system generates the following billing cause codes for this feature:
  - Outbound calls that are blocked due to seasonal suspend result in the billing cause code SERVICE_DENIED. Outbound calls that are redirected to the customer service number result in normal billing record events.

– Inbound calls that are blocked or redirected due to seasonal suspend result in billing cause code CALL_REJECTED.

Prerequisites

This section lists requirements that must be met before the feature can work.

Announcements

The appropriate announcements must be provisioned and available on the system, including announcements for generic seasonal suspend and DN referral. See release cause codes 1272 through 1275 and the associated announcements in the "Cause Code to Announcement ID Mappings" section of the *Cisco BTS 10200 Softswitch Provisioning Guide*. Routing to the announcement server must be working properly.

Note For features requiring an audible DN readout, such as seasonal suspend, the BTS 10200 has been tested for interoperability with the ThinkEngine Networks announcement server, Models 500X and 4000X.

VMA Treatment of Inbound Calls

This prerequisite applies if you are provisioning a customer with VMA treatment (instead of seasonal suspend treatment) for inbound calls.

The subscriber must have VMA activated and provisioned through the interactive voice response (IVR) provisioning system before you set the subscriber status to seasonal-suspend. If VMA is assigned and active, inbound calls to this subscriber are given VMA treatment instead of seasonal suspend treatment. However, outbound calls receive seasonal suspend treatment if status=seasonal-suspend.

Caution VMA, if assigned and active, takes precedence over the Seasonal Suspend feature. In this case, incoming calls *do not* receive seasonal suspend treatment. The incoming calls go directly to voice mail, and *not* to a seasonal suspend message, even if a seasonal suspend message is provisioned. Therefore, if the end user wishes to have seasonal suspend treatment for inbound calls, make sure that VMA is *deactivated* before setting status=seasonal-suspend.

Limitations

This section lists limitations for the Seasonal Suspend feature. These are conditions for which the Seasonal Suspend feature is not designed to work or works in a limited manner.

- This feature is not available to Centrex or multiline hunt group (MLHG) subscribers.
- The BTS 10200 does not support start and end timing for this feature.

Restrictions

This section lists restrictions. These are conditions that might cause this feature to fail or work improperly.

VMA Option

VMA, if provisioned and active, takes precedence over the Seasonal Suspend feature for treatment of inbound calls. The customer can call the VMA access DN (voice-mail pilot number) from any phone to use the voice-mail system. However, the following restrictions apply to calls placed from the seasonal subscriber line to the voice-mail pilot number:

- The customer can reach the voice-mail pilot number from the seasonal suspend phone only calling the pilot number directly. The customer cannot use a vertical service code (VSC) for this purpose, because VSCs do not work on a seasonal suspend line.
- If you want the customer to be able to dial the voice-mail pilot number, you must provision this pilot DN for white list treatment in the national-wb-list table and link this DN to the seasonal suspend cos-restrict table. See the applicable steps in the "Seasonal Suspend Provisioning for MR1.1 and Later" section in *Cisco BTS 10200 Softswitch Provisioning Guide*.

DN Readout by Announcement Server

Cisco has tested the ability of certain announcement servers to interwork with the BTS 10200 to provide DN-readout announcements. See the "Component Interoperability" section of the *Cisco BTS 10200 Softswitch Release Notes* for information on the capable announcement servers. Other announcement servers might also work, but might not have been tested for interoperability by Cisco.

Provisioning

For details on provisioning the "Seasonal Suspend feature for MR1.1 and Later", refer to *Cisco BTS 10200 Softswitch Provisioning Guide*.

Terminal and Group Make Busy Services

The Terminal Make Busy (TMB) and Group Make Busy (GMB) features enable the Cisco BTS 10200 Softswitch to give incoming callers the impression that specific terminals within a multiline hunt group (MLHG) or all members of the MLHG are busy. When you activate TMB or GMB, the BTS 10200 provides incoming callers with:

- A busy signal when the called directory number (DN) is associated with an MLHG when TMB is activated

or

- The next available number in the hunt sequence when a specific terminal DN within an MLHG is called and GMB is activated.

You can activate TMB for individual DNs or extensions within an MLHG, and you can activate GMB for the entire hunt group.

The BTS 10200 supports the following make busy services:

- Terminal Make Busy Activation (TMBA)
- Terminal Make Busy Deactivation (TMBD)

- Group Make Busy Activation (GMBA)
- Group Make Busy Deactivation (GMBD)

You activate and deactivate the TMB and GMB features by entering a vertical service code (VSC).

The BTS 10200 supports the TMB and GMB features for MLHG subscribers provisioned as any of the following subscriber types:

- MLHG
- MLHG-Individual
- MLHG-Pref-Individual
- CTXG-MLHG

For descriptions and definitions of the MLHG categories listed above, refer to *Multiline Hunt Group (MLHG)* in the *Cisco BTS 10200 Softswitch Network and Feature Descriptions Guide*.

TMB

You can assign the TMB feature to individual terminals associated with an MLHG by adding the feature to the MLHG and specifying the VSC, custom dial plan, and subscriber service. The subscriber activates and deactivates the feature by entering the appropriate vertical service codes.

When the subscriber activates TMB for a specific terminal, the BTS 10200 skips the terminal in the hunting sequence and gives the call to the next nonbusy terminal in the MLHG.

When the subscriber activates TMB for all terminals in the MLHG, the call is automatically given a busy tone or forwarded to voicemail if voicemail is provisioned.

The subscriber can originate calls from the terminal even if TMB is active.

GMB

Any subscriber within the MLHG that supports the GMB feature can activate or deactivate the feature. When GMB is active, the calling party receives a busy tone when dialing the MLHG pilot DN or main subscriber. None of the members of the MLHG receives the call and the hunt mechanism is disabled. If the subscriber has forwarding busy treatments such as Call Forward Busy (CFB) and voicemail activated, the BTS 10200 forwards the calls even with GMB activated.

The subscriber can originate calls from any terminal within the MLHG even if GMB is active.

Feature Interactions

The TMB and GMB features interact only with the CFB and voicemail features.

TMB

When TMB is activated for the subscriber, the BTS 10200 provides the calling party with an off-hook busy tone when they activate most features. The BTS 10200 disables Call Waiting (CW) and Caller ID on Call Waiting (CIDCW) for all MLHG customers. The system does not apply the CW tone on the pilot DN or MLHG terminals any time TMB is activated.

The BTS 10200 supports normal behavior for CFB and voicemail when TMB is activated. Refer to *Multiline Hunt Group (MLHG)* for additional information about MLHG features.

Table 3-9 and Table 3-10 provide examples of normal interactions between TMB and CFB.

CFB Is Active for Pilot DN And Terminals

Table 3-9 TMB—CFB Conditions and Actions: Pilot and Terminals

Called Number	Condition of Called Number	BTS 10200 Action
Pilot DN	Pilot busy	Hunt for next available terminal
	Pilot and all terminals busy	Call forwarded per CFB
MLHG terminal	MLHG terminal busy	Hunt for next available terminal
	All terminals busy	Call forwarded per CFB

CFB Is Active for Terminals Only

Table 3-10 TMB—CFB Conditions and Actions: Terminal Only

Called Number	Condition of Called Number	BTS 10200 Action
Pilot DN	Pilot busy	Hunt for next available terminal
	Pilot and all terminals busy	Busy tone
MLHG terminal	MLHG terminal busy	Hunt for next available terminal
	All terminals busy	Call forwarded per CFB

GMB

The BTS 10200 supports normal behavior for CFB and voicemail when GMB is activated.

Configuring

For details on configuring the TMB and GMB features, refer to *Cisco BTS 10200 Softswitch Provisioning Guide*.

Features for Centrex Subscribers Only

The Cisco BTS 10200 Softswitch provides Centrex-group functionality. A Centrex group is an emulation of a PBX by a Class 5 switch, and is typically assigned to a business group. The service provider can provision the values for the main subscriber of the Centrex group, and those properties are applied to the entire Centrex group. The service provider can also provision the parameters for simulated facility group (SFG) control, if SFG is desired. Both the incoming SFG (ISFG) and outgoing SFG (OSFG) are provisionable.

Tip To provision a Centrex group, see the Centrex Group provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

The following features are available to Centrex subscribers only:

- Call Hold (CHD), page 3-69
- Call Park and Call Retrieve, page 3-71
- Direct Inward/Outward Dialing for Centrex, page 3-71
- Directed Call Pickup (With and Without Barge-In), page 3-72
- Distinctive Alerting/Call Waiting Indication (DA/CWI), page 3-73

Call Hold (CHD)

The Cisco BTS 10200 Softswitch supports the call hold (CHD) feature as specified in LSSGR module FSD 01-02-1305 (TR-TSY-000579), *Add On Transfer And Conference Calling Features*.

Note This feature is available only to Centrex subscribers.

Description

The CHD feature allows the user to temporarily put an active call on hold and then make another call. The user can then return to the original call, and alternate between the two calls.

A party involved in an active call can use the CHD feature as follows:

- The user (the activating party) presses the **Flash** button or **hookswitch** and then presses the VSC for CHD (for example, ***52**).
- The network responds by putting the remote station on hold, providing silent termination. The system also returns a stutter dial tone to the activating party.
- If the activating party does nothing, the network waits 4 seconds, then removes the dial tone. In this case, the activating party can resume the call (recall the held party) by using the **Flash** button or **hookswitch**.
- If the activating party dials another remote station, then the system rings that station, and a new call is initiated if the remote station goes off hook.
- The CHD activation procedures (**Flash** button or **hookswitch** followed by the CHD VSC *52) can be used to toggle between the two calls. If the activating party disconnects while a party is on hold, the network responds by ringing the activating party's line. If the line is not answered within 6 ring cycles, the held party is disconnected. The held party does not hear an audible ringback during this ringing cycle.

Feature Interactions with CHD

The following feature interactions apply to CHD.

CHD and Emergency Number

There is an interaction when a Centrex subscriber invokes call hold (CHD) and places a call to an emergency number:

- When the emergency operator answers the call, a two-party call is active between the subscriber and the emergency operator. The on-hold party remains on hold.

- When the subscriber presses the Flash button or hookswitch, a three-way call is established among the subscriber, the emergency operator, and the previously on-hold party.
- It is not possible to place the emergency operator on hold.

CHD with CW/CIDCW and CFNA/VM/VMA

There is an interaction when a Centrex subscriber has all three of the following features assigned and active:

1. Call hold—CHD.
2. Call waiting—CW or CIDCW or both.
3. Call forwarding on no answer—CFNA, VM (or VMA), or any combination of these.

(Prior to Release 5.0 Maintenance Release 1.1) In this case, the system does not invoke forwarding for any incoming calls. If the subscriber wants to have the call-waiting features (CW or CIDCW) and call-forwarding features (CFNA, VM, or VMA) active simultaneously, the service provider should not assign the CHD feature to that subscriber.

(Release 5.0 MR1.1 and later) The system behavior is illustrated in the following example. In this example, CFNA is assigned and active on subscriber (A) along with CHD and CW.

- A and B are on an active call.
- C calls A.
- A hears the CW tone. (C hears ringback.)
- If A presses the **Flash** button or **hookswitch**, B is put on hold and A hears a dial tone.
- If A dials *52, A is connected to C.
- If A ignores the CW tone, C continues to hear ringback until the CFNA timer expires, then the call from C is forwarded per CFNA.

CHD and CFNA

If CHD is assigned to the subscriber (A) along with CFNA (CFNA active), the following interaction occurs.

- A and B are on an active call.
- C calls A.
- C hears a busy tone and is not connected. The call from C is not forwarded by the CFNA feature.

CHD and CW

If CHD is assigned to the subscriber (A) along with CW, the following interaction occurs.

- A and B are on an active call.
- C calls A.
- A hears the CW tone. (C hears ringback.)
- If A presses the **Flash** button or **hookswitch**, B is put on hold and A hears a dial tone.
- If A dials *52, A is connected to C.
- If A ignores the CW tone, C continues to hear ringback. The call is not forwarded.

Feature Provisioning

To provision this feature, see the CHD provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Call Park and Call Retrieve

Note This feature is available only to Centrex subscribers.

Call park (CPRK) and call retrieve (CPRK-RET) are defined for a call park subscriber group (CPSG), which is a subset of the Centrex subscriber group who have privileges to park and retrieve calls. Members of the CPSG can park and retrieve calls on a DN within their own CPSG. If desired, this feature can be used to transfer calls from one CPSG member to another.

CPRK allows a user in a business group to park an active call on a designated parking DN, leaving the user free to make other calls. The parked caller is placed on hold. The parking party is periodically reoffered the parked call. If the parking party accepts the reoffer attempt, or if another authorized user in the CPSG retrieves the call, then the call is connected. Otherwise, after three reoffer attempts, the call is released or forwarded as provisioned.

To park an active call:

- The parking party uses the **Flash** button or **hookswitch**, receives a recall dial tone, and dials the CPRK Access Code
- The parking party dials the DN of the desired CPSG member (or just hangs up or dials # to park the call against their own DN)
- A confirmation tone is provided to the parking party to confirm that the call is parked

To retrieve a parked call:

- The retrieving party dials the CPRK-RET access code and gets a dial tone
- The retrieving party dials the DN on which the call is parked
- The call is now connected between the calling party and the retrieving party

There is no deactivation procedure for this feature. The parked call is either connected or forwarded as described above.

Tip To provision this feature, see the CPRK provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Direct Inward/Outward Dialing for Centrex

Note This feature is available only to Centrex subscribers.

The Cisco BTS 10200 Softswitch supports the following direct inward/outward dialing features for Centrex systems as specified in LSSGR module FSD 01-01-1000 (TR-TSY-520), *Basic Business Group*:

- DID, including distinctive alerting and call-waiting tone—DID provides a Centrex group with the ability to receive a call from the PSTN without attendant intervention. The receiving Centrex station appears as a serving line to the CA. To provide a distinctive alerting and call-waiting tone, the service provider assigns the Distinctive Alerting/Call Waiting Indication (DA/CWI) feature to the subscriber.

Note For the distinctive call-waiting tones to be played, either the Call Waiting (CW) feature or the Call Waiting Deluxe (CWD) feature must also be assigned and active on the subscriber line.

- DOD provides a Centrex group with the ability to make a call to the PSTN without attendant intervention. The sending Centrex station appears as a serving line to the CA.

Directed Call Pickup (With and Without Barge-In)

Caution Do not provision this feature for subscribers other than Centrex subscribers. This feature will not work for subscriber other than Centrex Subscribers.

Directed call pickup allows a user in a basic business group (BBG) to answer a call to a telephone from another telephone in the BBG. There are two types of directed call pickup, with and without barge-in, each with its own activation access code. These codes are assigned by the administrator of the BBG, and can range from 2 to 65535.

The procedure for directed call pickup without barge-in (DPN) is as follows:

- The process begins when a telephone rings in the BBG, and a member of the BBG at a remote phone would like to pick up the call from the ringing telephone line
- At the remote telephone line, the user lifts the handset, and listens for a dial tone
- The remote user dials the DPN activation access code ***xx** (where xx represents the digits assigned for DPN activation in the BBG)
- The system returns a recall dial tone
- The remote user dials the extension associated with the ringing line
- The remote line is connected to the incoming call that actually terminated at the ringing line
- The original called line is now idle and available to originate and to receive calls
- If the incoming call has already been picked up by another member of the BBG, the additional DPN requests are routed to a reorder tone.

The procedure for directed call pickup with barge-in (DPU) is as follows:

- The process begins when a telephone rings in the BBG, is answered by the party, and another member of the BBG at a remote line wants to join the conversation
- At the remote telephone line, the user lifts the handset, and listens for a dial tone
- The remote user dials the DPU activation access code ***xx** (where xx represents the digits assigned for DPU activation in the BBG)
- The system returns a recall dial tone
- The remote user dials the extension on which the active call is taking place

- The system plays a confirming tone and establishes a three-way call (TWC) between the remote line and the original two parties
- The remote BBG user can press the **Flash** button or **hookswitch** to drop the other BBG party related to the original call
- If the remote BBG user goes on hook, the two-way connection will be reestablished between the calling party and the original BBG party

Tip To provision these features, see the DPN and DPU provisioning procedures in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Distinctive Alerting/Call Waiting Indication (DA/CWI)

Note This feature is available only to Centrex subscribers.

The distinctive alerting/call waiting indication (DA/CWI) feature is based on the Telcordia document *GR-520-CORE, Features Common to Residence and Business Customers I (FSDs 00 to 01-01-1110).* DA/CWI provides Centrex users special ringing and CW tones on DID calls. The Centrex administrator can activate this feature for some or all of the business group lines (BGLs) in the basic business group (BBG). Any call terminating at a designated BGL will receive the appropriate distinctive ringing or CW tone. When enabled, the subscriber can receive different ringing patterns (distinctive ringing) and CW alerting as follows.

- Calls originating within the same Centrex (also referred to as inside calls or extension dialing):
  - Ringing pattern: 2 seconds of ringing followed by 4 seconds of silence
  - CW pattern: 0.3-second beep
- Incoming calls originating outside the Centrex (outside calls, including calls from a *different* Centrex group):
  - Ringing pattern: 800 ms of ringing, 400 ms of silence, 800 ms of ringing, 4 seconds of silence
  - CW pattern: 0.1 seconds beep, 0.1 seconds silence, 0.1 seconds beep

Note For the distinctive call-waiting tones to be played, either the Call Waiting (CW) feature or the Call Waiting Deluxe (CWD) feature must also be assigned and active on the subscriber line.

Tip To provision this feature, see the DA/CWI provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Additional Features Applicable to Centrex and POTS

The following additional features are available to both Centrex and POTS subscribers:

- Anonymous Call Rejection (ACR), page 3-74
- Automatic Callback (AC)—Repeat Dialing, page 3-75

- Automatic Recall (AR)—Call Return, page 3-76
- Call Block - Reject Caller (CBLK), page 3-78
- Call Transfer (CT), page 3-79
- Change Number (CN), page 3-80
- Customer-Originated Trace (COT), page 3-80
- Do Not Disturb (DND), page 3-81
- Hotline Service, page 3-81
- Hotline-Variable Service (HOTV), page 3-82
- Interactive Voice Response (IVR) Functions, page 3-85
- Limited Call Duration Service (Prepaid/Postpaid) with RADIUS Interface to AAA, page 3-86
- Message Waiting Indicator (MWI)—Audible and Visual, page 3-89
- Multiline Hunt Group (MLHG), page 3-90
- Multiline Variety Package, page 3-105
- Multiple Directory Numbers (MDN), page 3-106
- No Solicitation Announcement (NSA), page 3-106
- Own Calling Number Announcement (OCNA), page 3-110
- Privacy Screening (Calling Identity with Enhanced Screening), page 3-111
- Speed Call, page 3-115
- Subscriber-Controlled Services and Screening List Editing (SLE), page 3-116
  - Selective Call Forwarding (SCF), page 3-117
  - Selective Call Acceptance (SCA), page 3-118
  - Selective Call Rejection (SCR), page 3-118
  - Distinctive Ringing/Call Waiting (DRCW), page 3-118
- Temporarily Disconnected Subscriber Status and Soft Dial Tone, page 3-119
- Three-Way Calling (TWC), page 3-121
- Three-Way Calling Deluxe (TWCD), page 3-122
- Usage-Sensitive Three-Way Calling (USTWC), page 3-127
- Voice Mail (VM) and Voice Mail Always (VMA), page 3-128
- Warmline Service, page 3-134

Anonymous Call Rejection (ACR)

The BTS 10200 supports the anonymous call rejection (ACR) feature as specified in LSSGR module FSD 01-02-1060 (TR-TSY-000567), *Anonymous Call Rejection.*

The ACR feature allows users to reject calls from parties that have set their privacy feature to prevent calling number delivery. When ACR is active the called party receives no alerting of incoming calls that are rejected. The incoming call is rerouted to a denial announcement indicating that private numbers are not accepted by the called party. To complete a call to the party with ACR, the calling party must enter

the VSC to activate calling identity delivery (for example, *82 for CIDSD) and then place a call to the party with ACR. Incoming calls to the called party with ACR are checked even if the called party is off hook.

If the BTS 10200 does not receive the calling party information in the incoming message, or if it does not receive the privacy setting in the incoming message, or if the privacy setting is unknown, the following process occurs. The system checks a provisionable parameter (PRIVACY-UNKNOWN-TREATMENT) in the Feature Configuration (feature-config) table. This parameter by default is set to PUBLIC, which means the incoming call is treated as public and is not rejected by the ACR feature. The service provider has the option to set this parameter to ANONYMOUS, which means the incoming call is treated as anonymous and is rejected by the ACR feature.

ACR has multiple activation options as follows:

- Activated permanently at subscription time by service provider.
- Activated by user:
  - The user lifts the handset, and listens for a dial tone.
  - The user presses the activation 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.

Tip To provision this feature, see the ACR provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Automatic Callback (AC)—Repeat Dialing

Automatic callback (AC), also called repeat dialing, allows the user to request the system to automatically redial the most recently dialed number. The system will keep attempting to call the number for up to 30 minutes. If the called party is busy when AC is activated, call setup is automatically performed when the called station becomes idle. The system alerts the calling party with distinctive ringing. Up to 20 AC requests can be active at any time. The service provider can set up this service for the user, or the user can access it on a usage-sensitive basis.

Note For intra-office AC with ARAC-TERMINATING-SPCS-SCAN-ALLOW;VALUE=Y, the feature operates as expected during a Feature Server switchover. However, for inter-office AC with the same switchover condition, the feature fails because TCAP is not replicated.

AC is activated as follows:

- The user calls a remote station, receives a busy signal or no answer, and hangs up.
- The user lifts the handset again, and listens for dial tone.
- The user enters the VSC for AC activation (for example, ***66**). One of the following scenarios will occur:
  - Audible ring—Indicates that the call setup is being attempted immediately.
  - The delayed processing announcement—This announcement is given to indicate that the line the customer is calling is busy and that the system will attempt to complete the call when the called line is idle.
  - A short term denial announcement, such as "We are sorry. Your AC request cannot be processed at this time. Please try again later or dial directly."
  - A long term denial announcement, such as "The number you are trying to reach cannot be handled by AC. Please dial directly."
  - A denial announcement, such as "The called party has a call rejection feature active and is not accepting calls from you."

AC is deactivated as follows:

- The user goes off hook, receives a dial tone, and dials the deactivation code (for example, ***86**).
- Once the deactivation code is dialed the user hears an announcement stating that all outstanding AC requests have been deactivated.

Note The AC feature can be made available to all subscribers lines connected to a BTS 10200 using the default office service ID, or to all subscribers in a specific POP using the office service ID. See the "Office Service ID and Default Office Service ID" section on page 3-134 for a general description of this provisionable service.

Tip To provision this feature, see the AC provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Automatic Recall (AR)—Call Return

Automatic Recall (AR), also called call return, allows the user to request the system to automatically redial the DN of the last incoming call (that is, the station that called the user). The AR subscriber does not need to know the telephone number or the calling party of the last incoming call. If the remote party is busy when AR is activated, the system continues attempting to call the number for up to 30 minutes, and automatically performs call setup when the called station becomes idle. The system alerts the calling party (the party that initiated the AR) with distinctive ringing. Up to 20 AR requests can be active at any time.

The service provider can set up the AR feature on a system-wide or POP-wide basis, or the user can access it on a usage-sensitive basis.

There are two variants of AR feature activation, one-level and two-level. With one-level activation, the user activates the AR feature without knowing the last calling party number. With two-level AR activation, the user hears a voice announcement of the last incoming calling party number, the date and time when the call was received, and a voice instruction for activating an AR call to that party.

Reference: LSSGR module FSD 01-02-1260 (GR-227-CORE), *Automatic Recall.*

Note For intra-office AR with ARAC-TERMINATING-SPCS-SCAN-ALLOW;VALUE=Y, the feature operates as expected during a Feature Server switchover. However, for inter-office AR with the same switchover condition, the feature fails because TCAP is not replicated.

One-Level Activation of AR

One-level AR is activated as follows:

- The user receives a call (ringing) from a remote station, but does not pick up.
- The user lifts the handset and listens for dial tone.
- The user enters the VSC for activation (for example, ***69**). One of the following scenarios will occur:
  - Audible ring—Indicates that the call setup is being attempted immediately.
  - The delayed processing announcement—This announcement is given to indicate that the line the customer is calling is busy and that the system will attempt to complete the call once the called line is idle.
  - A short term denial announcement, such as “We are sorry. Your AR request cannot be processed at this time. Please try again later or dial directly.”
  - A long term denial announcement, such as “The number you are trying to reach cannot be handled by AR. Please dial directly.”
  - A denial announcement, such as “The called party has a call rejection feature active and is not accepting calls from you.”

AR is deactivated as follows:

- The user goes off hook, receives a dial tone, and dials the deactivation code (for example, ***89**).
- Once the deactivation code is dialed the user hears an announcement stating that all outstanding AR requests have been deactivated.

Two-Level Activation of AR

Two-Level AR activation is an extension of the one-level AR feature. It requires communications with an IVR server, which delivers the voice readout of the calling-party number, provides appropriate voice prompts, and collects the user’s response.

- First stage—The user dials the activation code (for example, *69) and hears a voice announcement of the last incoming calling party number, the date and time when the call was received, and a voice instruction for activating an AR call to that party. The user can hang up to discontinue AR activation toward that party.
- Second stage—If the subscriber follows the instruction and presses “1”, the system activates the AR call.

Note During the second stage, the system automatically checks for invalid digits and timeouts.

The deactivation procedure for two-level AR is the same as for one-level AR.

Note The AR feature can be made available to all subscribers lines connected to a BTS 10200 using the default office service ID, or to all subscribers in a specific POP using the office service ID. See the "Office Service ID and Default Office Service ID" section on page 3-134 for a general description of this provisionable service.

Tip For more details about the IVR interactions for this feature, see Chapter 6, "Interactive Voice Response Functions."

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the AR provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Call Block - Reject Caller (CBLK)

The call block (CBLK) feature, also referred to as the reject-caller feature, allows the user to block incoming calls from the DN of the last received call. For the call block feature to work, the user must already be subscribed to the selective call rejection (SCR) feature. Once call block is activated against a specified DN, that DN remains in the SCR list of the subscriber. A subscriber who wishes to block callers (like sales calls, etc.) but does not know the caller's DN, can use this feature. Call block can be provided to POTS, Centrex, and MLHG subscribers.

Provisioning call block includes the following CLI operations:

- Configuring the feature table for call block
- Provisioning a two-digit star code (*xx) for call block activation:
  - Adding a star code entry in the VSC table (for POTS subscribers)
  - Adding a star code entry in the custom dial plan table (for Centrex subscribers)
- Creating a service with call block and SCR
- Assigning the service to the subscriber via the subscriber service profile table

An idle user (if subscribed to SCR) can dial the call block activation code indicating that the last incoming caller's DN is to be added to their SCR list.

A confirmation tone is given to indicate successful activation. In cases of error or the user not subscribed to call block, a reorder tone is given. If the user is trying to activate call block while on an active call, the user is reconnected to the original call.

The user can deactivate call block for this DN by removing the DN from their SCR list. This is done by using the screen list editing (SLE) function of the SCR feature.

Note For details of the SCR feature, see the "Selective Call Rejection (SCR)" section on page 3-118.

Tip To provision this feature, see the CBLK provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Block All Inbound Calls

If the subscriber has blocked all the inbound calls, the calling party hears an announcement stating that called party has chosen to deny all inbound calls.

Note A personalized announcement can be provided by provisioning an announcement ID specifically defined for the subscriber. Use the announcement ID 800 through 899 for custom announcements.

Tip To provision this feature, see the Block All Inbound Calls provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Call Transfer (CT)

The Cisco BTS 10200 Softswitch supports the call transfer (CT) feature as specified in LSSGR module FSD 01-02-1305 (TR-TSY-000579), *Add On Transfer And Conference Calling Features*.

CT allows a user to add a third party or second call to an existing two-party call. CT also allows the user to hang up while involved in the two calls and connect the remaining two parties in a two-way connection.

To activate a CT call, a user (A) involved in a stable two-way call (with B) takes the following steps:

- User A (the initiating party) presses the **Flash** button or **hookswitch**. This places the remote end (B) on hold and returns a recall dial tone.
- User A dials the DN of the third party (C).

Note If A presses the **Flash** button or **hookswitch** before completing dialing, the original two-way connection is reestablished between A and B.

- When C answers, only A and C can hear and talk. This allows A to speak privately with C before sending the second flash.
- If A presses the **Flash** button or **hookswitch** after successfully dialing C, a three-way conference is established regardless of whether C answers the call.

The following scenarios occur, depending upon the actions of the parties in the call:

- If A hangs up after successfully dialing C (C is ringing), a two-way call is established between B and C, regardless of whether C answers the call. User A is billed for a call transfer and is also billed for the duration that the other two parties are on the call.

- If A waits until C answers the call, and then A hangs up, a two-way call is established between B and C. User A is billed for a call transfer and is also billed for the entire duration starting from the time A initiated the TWC until B and C hang up.

Feature Provisioning Commands

To provision this feature, see the CT provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

SIP Call Transfer with REFER and SIP Invite with REPLACES

Call transfer is performed by SIP systems through the following features:

- SIP call transfer with REFER
- SIP Invite with REPLACES

For information on these features, see the "SIP Call Transfer with REFER and SIP Invite with REPLACES" section in the *Cisco BTS 10200 Softswitch SIP Feature and Provisioning Guide*.

Change Number (CN)

The change number (CN) feature, also refered to as the call referral feature, enables the service provider to change the directory number of a subscriber. In addition, the Change Number feature provides a mechanism to track the last time and date a call referral number change announcement was activated or requested in association with a subscriber phone number change or disconnect. This allows the service provider to query the subscriber number changed status in the BTS 10200 system in order to find out how long the number changed announcement (call referral) has been active for the subscriber. The call referral announcement is activated when a phone number is disconnected or changed. An announcement is played when someone calls the number indicating that the number has been disconnected or; if changed, indicating that the new number is xxx-xxx-xxxx. If there is no new phone number, a generic announcement is played indicating only that the number has changed or has been disconnected. Either type of announcement will be played until disabled by the service provider. To change the directory number of a subscriber and to setup and disable the call referral announcements, refer to the "Managing Subscribers" section of the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

Customer-Originated Trace (COT)

Customer-originated trace (COT) allows users who have been receiving harassing or prank calls to activate an immediate trace of the last incoming call, without requiring prior approval or manual intervention by telephone company personnel.

After a harassing or prank call is terminated, a user who wishes to trace the call goes off hook, receives a dial tone, and dials the COT activation code (for example, *57). When the trace has been completed, the user receives a COT success tone or announcement, such as, "You have successfully traced your last incoming call. Please contact your telephone company for further assistance." (Information about a traced call is made available to the telephone company or to a telephone company-designated agency, usually law enforcement, but not to the user who initiated the trace). Because COT is activated on a per-call basis, the service is deactivated when the user goes on hook.

If the trace cannot be performed, an appropriate tone or announcement is played. COT is inhibited on the following subscriber categories:

- PBX
- RACF
- IVR
- CTXG_TG

Note For an incoming call to be traced, the incoming call must have been answered by the called party.

All COT trace records are stored in the EMS of the BTS 10200 for retrieval purposes. A maximum of 10,000 traces are stored in a circular file format (oldest record overwritten).

Note The COT feature can be made available to all subscribers lines connected to a BTS 10200 using the default office service ID, or to all subscribers in a specific POP using the office service ID. See the "Office Service ID and Default Office Service ID" section on page 3-134 for a general description of this provisionable service.

Tip To provision this feature, see the COT provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Do Not Disturb (DND)

The do not disturb (DND) feature, when activated, blocks all incoming calls to the subscriber line. This feature can be activated and deactivated by the individual user via the handset. DND routes incoming calls (calls destined for the user's DN) to a DND announcement. When a call comes in to a line on which DND is active, the called party receives a reminder ring (provided the service provider has provisioned the DND feature with reminder ring enabled). The user is not able to receive the call. A user can enter the activation code (for example, *78) on the handset to enable this service, and the deactivation code (for example, *79) to disable the service.

Note The reminder ring cannot be used with SIP devices.

Tip To provision this feature, see the DND provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Hotline Service

Hotline service is a dedicated private line between a subscriber phone and a predetermined DN. The service is activated by the service provider at the request of the subscriber. When the hotline user picks up the phone, the Cisco BTS 10200 Softswitch rings the predetermined DN instantly.

An exclusive telephone DN is required for the hotline feature, and certain limitations apply to its use:

Certain limitations apply to the use of the hotline feature:

- An exclusive telephone DN is required for the hotline feature.
- None of the VSC star (*) features are available on this line

Only the service provider can deactivate hotline service.

Note See also the "Warmline Service" section on page 3-134. Warmline service is a combination of hotline service and regular phone service.

Tip To provision this feature, see the Hotline provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Hotline-Variable Service (HOTV)

This section describes the hotline-variable feature.

Hotline-Variable Feature Description

Hotline-variable service allows the user to go off hook, receive dial tone, and let the system call a specified DN automatically after a dial-tone timeout. The service provider provisions the hotline-variable dial-tone timeout for the system (default is 4 seconds) and assigns the hotline-variable feature to individual subscribers. The user activates the hotline-variable service on his or her line and specifies the remote DN using the handset. Once activated, the service works as follows:

- Use of hotline-variable for regular calling—The user takes the handset off hook, receives dial tone, and starts dialing a regular call before the dial-tone timeout expires.
- Use of hotline-variable as a hotline—The user takes the handset off hook, receives dial tone, but does not dial any digits. After the dial-tone timeout expires, the system automatically calls the user-specified DN.

Caution The HOTV feature operates only with MGWs that are compliant with MGCP1.0 (per IETF document *RFC 2705*) or higher. It is not supported on MGCP0.1 MGWs.

The following conditions and limitations apply to the hotline-variable feature:

- The hotline-variable feature can be provided to POTS, Centrex, and MLHG subscribers.
- The hotline-variable feature is in the deactivated mode unless activated by the subscriber. Once activated, the feature remains in the activated mode until deactivated.
- None of the VSC star (*) features are available on this line, other than the VSC codes for hotline-variable activation, deactivation, and interrogation.

This remote DN is referred to as the B-number. The allowed types of B-numbers are listed in Table 3-11.

Table 3-11 Allowed Types of B-numbers

Subscriber Type	Allowed B-number
POTS	DN, without extensions
Centrex	Public access code + external DN, without extensions
	An extension within the business group

The hotline-variable feature is composed of four associated features, which are described in the sections that follow:

- Hotline-Variable Activation, page 3-83
- Hotline-Variable Deactivation, page 3-83
- Hotline-Variable Interrogation, page 3-83
- Hotline-Variable Invocation, page 3-84

Hotline-Variable Activation

Hotline-variable activation allows a user to activate the hotline function on his or her local phone. The user does this by going off hook and receiving dial tone, then dialing *52*B-number#, where:

- *52* is an example of the activation VSC for HOTV (VSCs are provisionable by the service provider)
- B-number is the remote DN that the user wants to reach via hotline calling
- # is a trailing symbol that identifies the end of B-number digits

A success announcement is given on a successful activation, and an error announcement indicating the type of error is given if activation is unsuccessful.

The system screens the DN entered for the B-number, and denies the activation attempt if any of the following conditions apply:

1. The call type is restricted in the NOD-RESTRICT-LIST table for HOTV
2. The call is restricted for the subscriber by the OCB feature
3. HOTV is already activated

A successful activation results in overwriting the previous DN recorded for hotline-variable.

Hotline-Variable Deactivation

Hotline-variable deactivation allows a user to deactivate hotline-variable on his or her local phone. An example of a dial string for hotline-variable deactivation is #52#. A success announcement is given on a successful deactivation, and an error announcement, indicating the type of error, is given if deactivation is unsuccessful.

Hotline-Variable Interrogation

Hotline-variable interrogation allows a user to check whether hotline-variable is activated to a particular remote phone. An example of a dial string for hotline-variable interrogation is *#52*B-number#. A success announcement is given to the user if hotline-variable is activated to the B-number. If

hotline-variable is not activated, or if hotline-variable is activated to a different phone, an appropriate error announcement will be provided to the user. If the user has hotline-variable activated to the B-number, a success announcement is provided. Otherwise an error announcement is provided.

Note If the user enters a digit string that does not match exactly the B-number against which hotline-variable was activated, the interrogation attempt will result in an error announcement.

Hotline-Variable Invocation

Hotline-variable invocation is the actual procedure the system follows when the user goes off hook, provided that the feature is subscribed and activated. If the user begins dialing digits before the dial-tone timeout period expires, the system attempts to complete the call to the dialed DN. If the user dials no digits until the dial-tone timeout period expires, the system automatically calls the predetermined hotline destination B-number.

Invalid User Actions

The valid user actions are described in the sections above. The following user actions are invalid, and the system provides an appropriate error announcement:

- The user enters an invalid directory number (DN) for the B-number.
- During HOTV activation, the user enters a B-number that is determined by the FS to be a call type blocked by provisioning in the NOD-RESTRICT-LIST table. For example, the nature of dial (NOD) from the user's phone to the B-number is an emergency call, but emergency calls are blocked by provisioning in the NOD-RESTRICT-LIST table.
- The user tries to activate hotline-variable from a DN that has outgoing calls blocked by the OCB feature, or the user enters a B-number, but calls to that DN are blocked by OCB. For example, the call from the user's phone to the B-number would be a domestic long distance call, but these calls are blocked by setting K=2 against the OCB feature in the SUBSCRIBER-FEATURE-DATA table.
- The user tries to activate hotline-variable to an international DN, but the service provider has blocked forwarding to international DNs. The service provider can block forwarding to international DNs using the OCB feature.
- The user tries to activate hotline-variable when already activated (the B-number is not overwritten).
- The user tries to activate hotline-variable to his or her own extension or DN.
- The user tries to deactivate hotline-variable when already deactivated.
- The user interrogates hotline-variable, but enters a digit string that does not match exactly the B-number against which hotline-variable was activated. For example, if hotline-variable was activated with a 5-digit string corresponding to a Centrex extension, and interrogation is attempted using a 10-digit string of the complete DN, the interrogation attempt will result in the applicable announcement. (See the complete list of standard Cisco BTS 10200 announcements in the *Cisco BTS 10200 Softswitch Provisioning Guide*.)
- The user tries to interrogate hotline-variable on a fresh system (a system with no entry in the SUBSCRIBER-FEATURE-DATA table). In this case, the user receives the error announcement immediately after entering the VSC (for example, *#52*). The system does not wait for the user to enter the B-number.

HOTV Feature Interactions

HOTVA and OCB—If the user tries to activate hotline-variable to a DN, but calls to that DN are blocked by OCB, the activation is denied, and the user receives an error announcement.

HOTV and OCB—If the user has already activated hotline-variable successfully to a DN, and then restricts calls to this DN via the OCB feature, future hotline-variable calls will be denied, and an error announcement will be provided to the user.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

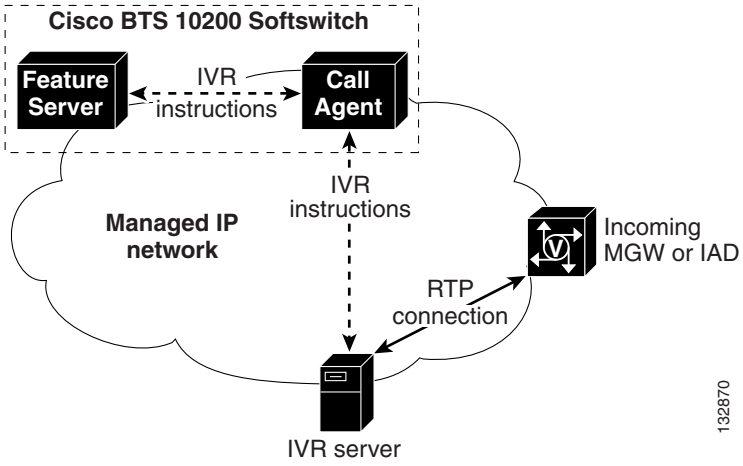
Tip To provision this feature, see the HOTV provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Interactive Voice Response (IVR) Functions

The system supports interactive voice response (IVR) functions through an external IVR server deployed in the service provider network. IVR functions are used with several of the subscriber features, including RACF, two-level AR, SCA, SCF, SCR, and NSA.

To begin an IVR session for the subscriber, the BTS 10200 establishes an RTP connection between the IVR server and the incoming gateway (a MGW or integrated access device, IAD). This connection is illustrated in Figure 3-2.

Figure 3-2 IVR Connections



Following is the call scenario for IVR.

Note During this process, the Feature Server (FS) and Call Agent (CA) exchange IVR instructions as needed.

1. The incoming call arrives at the incoming gateway (MGW or IAD).
2. The CA sets up an RTP connection between the IVR server and the incoming gateway.

3. The IVR server communicates with the gateway and sends the IVR result to the CA.
4. The CA stops the IVR connection.

The following limitations apply to IVR functions:

- The feature is not supported for SS7, H.323, or SIP endpoints.
- The BTS 10200 does not support local IVR capability. Instead it relies on IVR capabilities provided from an external IVR server supporting the MGCP BAU package.
- For IVR trunk groups, LOCAL-TRUNK-SELECTION is not used.
- The IVR-based COS feature (used for account and authorization codes) is supported only for ISDN PRI trunks and only in the North American market. For details of this application, see the "Account Codes and Authorization Codes" section on page 4-7.

The IVR operations for each subscriber feature are described in Chapter 6, "Interactive Voice Response Functions."

The system provides Multi-Lingual Support (MLS) for IVR and announcement services. This allows subscribers to select a preferred language (English, French, or Spanish) in which to hear the IVR prompts. See the "Multi-Lingual Support Feature" section on page 6-45.

To set options for IVR prompts, see the Class of Service (COS) provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

To provision IVR support for features that use the IVR functionality, see the applicable feature provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Limited Call Duration Service (Prepaid/Postpaid) with RADIUS Interface to AAA

This section describes the BTS 10200 support for the Limited Call Duration (LCD) feature, including both prepaid and postpaid services. This support includes interfaces to an authentication, authorization, and accounting (AAA) server. The LCD feature can be assigned to any BTS 10200 subscriber with any phone type, including Media Gateway Control Protocol (MGCP)-based, Session Initiation Protocol (SIP)-based, and network-based call signaling (NCS)-based phones.

This section also lists the interactions of this feature with other subscriber features.

Network Interfaces

The BTS 10200 uses the following signaling interfaces for this feature:

- RADIUS-based interface to an AAA server. The feature uses RADIUS Access Request and Account Request messages.
- Additional interfaces for call-control signaling, including communications with MGCP-based and TGCP-based media gateways (MGWs), IP Transfer Points (ITPs) via SIGTRAN (for SS7), and PacketCable-based CMTSs and eMTAs.
- SFTP interfaces to external third-party billing servers for transfer of billing records, and RADIUS interfaces to external record keeping servers (RKSs) for transfer of PacketCable-based event messages (EMs).

Feature Description

The LCD feature supports both prepaid and postpaid services for subscribers.

- Fixed-prepaid (debit) service is an outgoing call management feature that allows a subscriber to pay for call charges in advance. Each time the subscriber makes a call, the charges for the call are deducted from the balance of the advance payment. If the subscriber uses up all of the advance payment, the BTS 10200 blocks all further calls from this subscriber (until more money is added to the account).
- Postpaid-with-limit (credit) service is an outgoing call management feature that limits the calls originated from the subscriber so that total outstanding balance of charges for all the calls originated from the subscriber is less than a predefined limit. If the subscriber reaches the predefined limit, the BTS 10200 blocks all further calls from this subscriber (until money is paid on the account or the limit is increased).

When a subscriber with the LCD feature originates a call, the BTS 10200 contacts a designated prepaid AAA server via a RADIUS interface, and requests authorization to provide service for the subscriber. If the subscriber is allowed to make the call, the AAA server sends a success response to the BTS 10200. The response includes the call duration quota and the billing model of the subscriber (credit or debit). The BTS 10200 uses normal routing mechanisms to route the call. If the call continues beyond the allocated quota, the BTS 10200 tries to reauthorize the call with the AAA server. The call continues until it is either released by the calling or called party, or an attempt to reauthorize fails. If a reauthorization attempt fails, the BTS 10200 attempts to send a warning tone to the calling subscriber just before it is forcibly released.

If the AAA server rejects the authorization or authentication of the call, the system takes appropriate action depending on the value of the return code received from AAA server. If the system cannot authorize/authenticate a call due to a failure of communication with the AAA server, the call is released with an announcement.

The system applies LCD screening (authorization/authentication) to all nonemergency calls originated by a subscriber with the LCD feature assigned, unless the service provider has specifically provisioned the type of call to be excluded from screening.

The system never applies LCD screening to emergency calls (calls to numbers that are set to call-type=EMG in the Destination table) even if the LCD feature is assigned to the subscriber. LCD subscribers will be allowed to make calls to emergency numbers regardless of the balance in their account.

Provisionable Parameters

A new provisionable subscriber feature, Limited Call Duration (LCD), is added in this release to support prepaid features. It generates a trigger, LCD_TRIGGER, at the COLLECTED_INFORMATION trigger-detection point.

Feature Interactions

Calls to emergency numbers will not be authenticated even if the LCD feature is assigned to the subscriber. Therefore, LCD subscribers will be able to make emergency calls regardless of the balance in their account. From the implementation perspective, the system will not generate an LCD trigger if the call-type is emergency (EMG).

Note If you are using separate directory numbers (DNs) for ambulance, fire, and police service (typically applies to networks outside the United States), Cisco strongly recommends that you provision these as call-type=EMG and call-subtype=<AMBULANCE or FIRE or POLICE> in the Destination table. This is the only way to be sure that calls to these DNs will be given the priority treatment of the EMG call-type for all features.

All nonemergency calls, including toll-free calls, originated by a subscriber with the LCD feature will undergo authorization/authentication unless explicitly provisioned not to do so in the Trigger Nature of Dial Escape List (trigger-nod-escape-list) table.

LCD will have a higher precedence than Local Number Portability (LNP).

All types of forwarded calls (CFU, CFNA, CFB, and CFC) from the LCD subscriber will undergo the authorization/authentication and will be subject to the maximum available quota. However, the system does not perform authentication for calls redirected from the subscriber to the voice-mail application server.

If the subscriber has an Outgoing Call Barring (OCB) feature and LCD feature, the authorization/authentication will be done only if the call is not blocked; that is, OCB takes precedence over LCD.

Class of Service restriction will take precedence over the LCD feature.

Hotline/Warmline/HOTV features will undergo the authorization/authentication and will be subject to the maximum available quota.

Speed Call/Abbreviated Dial calls originated by the subscriber with the LCD feature will undergo the authorization/authentication and will be subject to the maximum available quota.

Each leg of the call originated by the LCD subscriber in a TWC and TWC Deluxe will undergo the authorization/authentication and will be subject to the maximum available quota.

Each leg of the call originated by the LCD subscriber during call transfer will undergo the authorization/authentication and will be subject to the maximum available quota.

The Call Waiting feature will be supported for the LCD subscriber. This includes scenarios where both the calls are terminating calls to the LCD subscriber and a scenario where only one of the calls is the terminating call to the LCD subscriber.

Authorization/authentication will not be done for Vertical Service Code (VSC) features, except when a courtesy call is required for certain VSC features, such as Call Forwarding Unconditional Activation (CFUA) and Call Forwarding Variable for Basic Business Group Activation (CFVABBG).

Authorization/authentication will not be done for Centrex subscriber originating calls; that is, the LCD feature is not supported for Centrex subscribers.

The system does not perform authorization/authentication for calls sent to the interactive voice response (IVR) server.

The system does not perform authentication for calls sent from the privacy screening (PS) application server to the subscriber.

Prerequisites

The implementation of the LCD feature in the BTS 10200 is based on the standards listed below. To interwork with the BTS 10200, the external AAA server must support these same interface requirements.

- All the standard attributes used in this implementation conform to the Internet Engineering Task Force (IETF) documents RFC 2865, 2866, and 2869. (The system is capable of accepting additional RADIUS attributes that conform to these RFC documents, but does not process these attributes.)
- All of the vendor-specific attributes (VSAs) used in this implementation conform to the definitions in the *RADIUS VSA Voice Implementation Guide* at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.pdf

Note If you need a complete compliance matrix, contact your Cisco account team for details.

Restrictions and Limitations

If a reauthorization attempt fails, the BTS 10200 attempts to send a warning tone to the calling subscriber just before it is forcibly released. However, the system may not be able to send the warning tone if the subscriber is using a SIP phone.

The LCD feature is not supported for H.323 subscribers in this release.

Note The LCD functionality of the BTS 10200 has been tested with the MIND C.T.I. iPhonEX as the AAA RADIUS server.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the LCD provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Message Waiting Indicator (MWI)—Audible and Visual

The BTS 10200 supports both audible message waiting indicator (MWI), also called stutter dial tone (SDT), and visual message waiting indicator (VMWI). These indicators are associated with voice mail service. When a call is forwarded to a voice mail system, and the caller leaves a message or retrieves all pending messages, the voice mail server sends a message to the Cisco BTS 10200 Softswitch with voice mail status information. In response to this, the Cisco BTS 10200 Softswitch notifies the voice mail status (on/off) to the called party (subscriber) by sending the appropriate signaling message to the MGCP/NCS residential gateway.

- If the MWI feature is enabled for the subscribe (as configured in the SDT-MWI field in the SUBSCRIBER table), a SDT is delivered when the phone goes off hook and the subscriber has unretrieved voice mails.
- If the VMWI feature is enabled for the subscriber (as configured in the VMWI field in the SUBSCRIBER table), and the subscriber has unretrieved voice mails, the telephone indicator light turns on. After the subscriber retrieves all voice mails, the indicator light turns off.

Note For the MWI feature to be enabled for the subscriber and deliver the SDT when the phone goes off hook, MWI must be enabled at the MGW profile level (MGCP-MWI-SUPP field in the MGW-PROFILE table) *and* SDT must be enabled at the subscriber level (SDT-MWI field in the SUBSCRIBER table).

Similarly, for VMWI to be enabled for the subscriber and turn the indicator light on, the VMWI feature must be enabled at the MGW profile level (MGCP-VMWI-SUPP field in the MGW-PROFILE table) *and* the subscriber level (VMWI field in the SUBSCRIBER table).

The signaling details are as follows:

- For MWI, the BTS 10200 sends the RQNT message to the MGW containing S:L/mwi when the subscriber goes off hook and a message is waiting for the subscriber.
- For VMWI, the BTS 10200 sends the RQNT message to the MGW containing S:L/vmwi(+) when a message is left for the subscriber. This message is sent regardless of whether the phone is off hook or on hook.
- After the subscriber retrieves all voice mail messages, the BTS 10200 sends the RQNT message to MGW with S:L/vmwi(-).

The service provider can display and reset a subscriber's MWI status through the use of CLI commands. The **status subscriber** command displays the current MWI status, and the **control subscriber** command can be used to turn the MWI status on or off.

Tip For information on provisionable options for customer access to voice mail, see the "Voice Mail (VM) and Voice Mail Always (VMA)" section on page 3-128.

Multiline Hunt Group (MLHG)

The Cisco BTS 10200 Softswitch supports multiline hunt group (MLHG) features. An MLHG is a collection of lines organized into a group with a single pilot DN (also referred to as the group DN or the main-subscriber DN). Optionally, individual DNs can be assigned to some or all of the lines in the group. Each line in an MLHG has a terminal number that identifies its position in the group. When there is an incoming call, if the first line in the MLHG is busy, the next line is hunted and so on until an idle line is found.

Reference: LSSGR module FSD 01-02-0802 (GR-569-CORE), *Multiline Hunt Service.*

Note The MLHG feature is supported only for MGCP and NCS subscribers.

Hunting Sequence

The system hunts for an idle line by means of a defined search sequence. The sequence is specified by the provisioning of the hunt-type parameter in the MLHG table—regular, circular, or uniform call distribution (UCD). The system also supports preferential hunt lists.

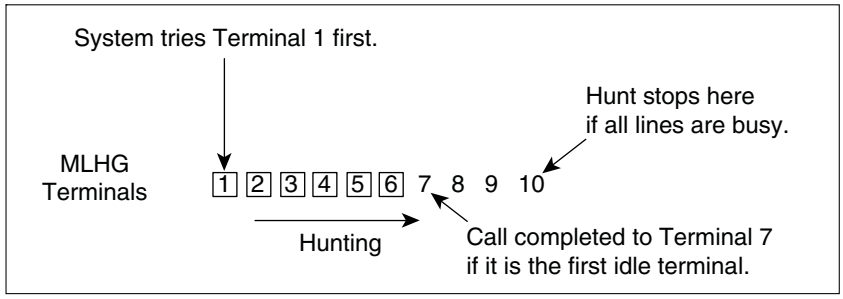
The starting point for the hunt depends upon whether the incoming call is being routed to the group or to the individual. These scenarios are described in the following sections:

- Incoming Call to the Pilot DN, page 3-90
- Incoming Call to an Individual DN, page 3-92

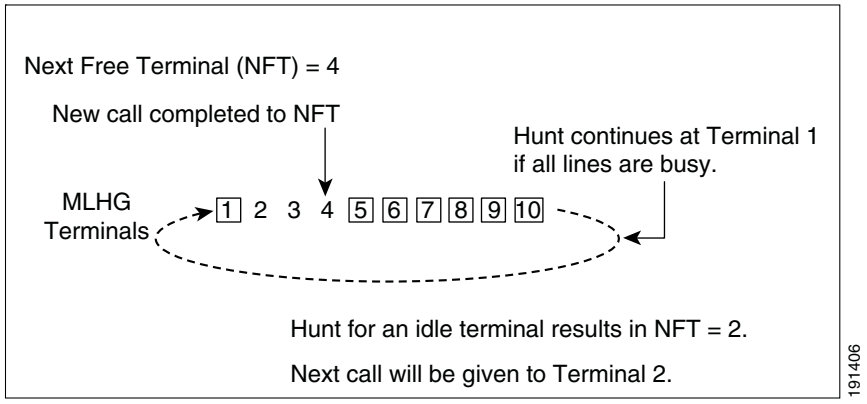
Incoming Call to the Pilot DN

If the dialed digits of the incoming call match the DN for the main-sub-id (the pilot DN), the call is routed to the group. Figure 3-3 illustrates this process.

Figure 3-3 Searching an MLHG—Incoming Call to the Pilot DN (Example)



Regular hunt and circular hunt



UCD hunt

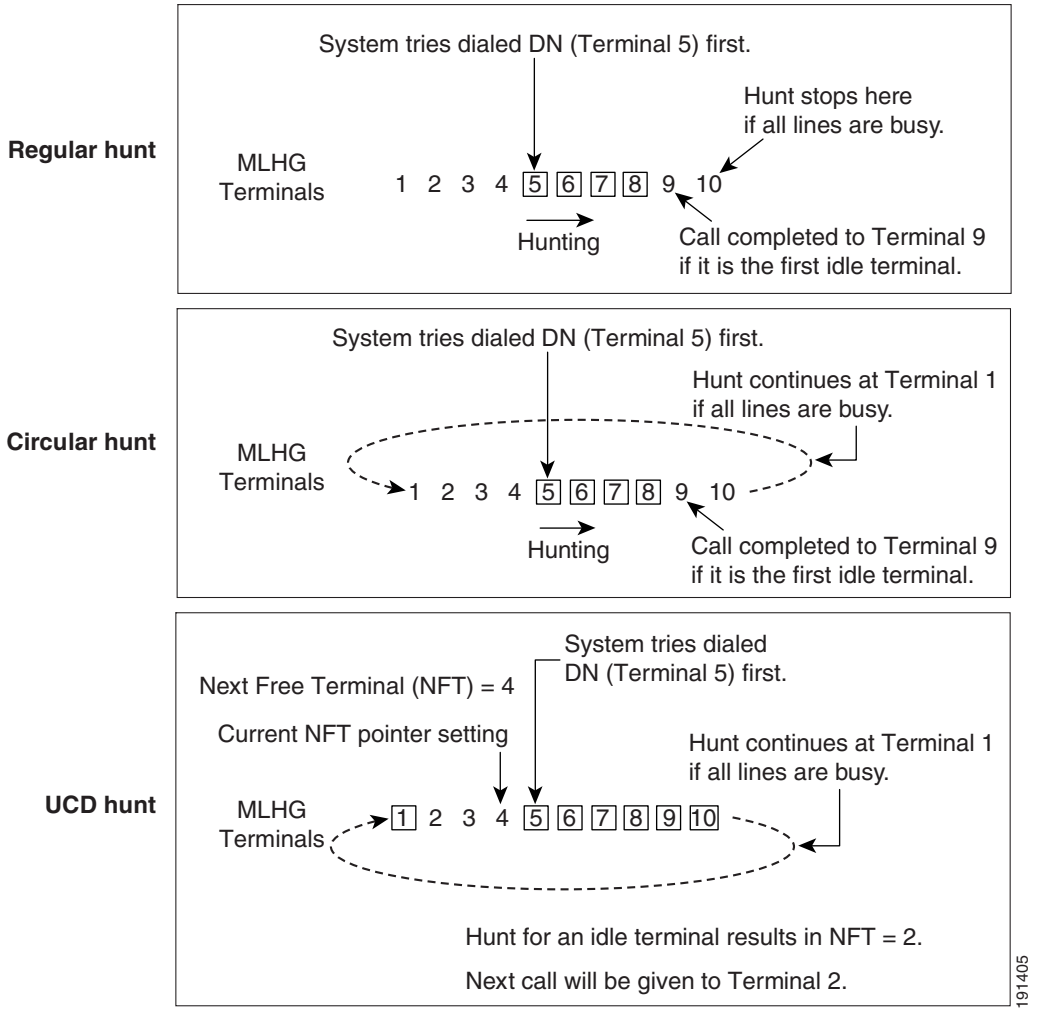
Notes for Figure 3-3

- A rectangle surrounding a number means the line is busy.
- Regular hunt and circular hunt (the hunting treatment for regular hunt and circular hunt are identical when the pilot DN is dialed)—The incoming call is routed to Terminal 1. If Terminal 1 is busy, the system hunts for the next idle terminal. If none of the terminals (2 through 10) is available, the hunt ends and the system does not answer the call.
- UCD hunt—From previous calls, the system has set the next-free-terminal (NFT) pointer to Terminal 4. Therefore the call is completed to Terminal 4. When the call is completed to Terminal 4, the system sets the NFT pointer to the next idle line (Terminal 2). The system will give the next call to Terminal 2.

Incoming Call to an Individual DN

If the dialed digits of the incoming call match the DN for an individual terminal, the call is routed to that specific terminal. However, if that terminal is busy, the system hunts for an idle line. Figure 3-4 illustrates this process.

Figure 3-4 Searching an MLHG—Incoming Call to an Individual Terminal (Example)



Notes for Figure 3-4

- A rectangle surrounding a number means the line is busy.
- Regular hunt—The incoming call is routed to the terminal with the dialed DN, Terminal 5 in this example. If Terminal 5 is busy, the system hunts for the next idle terminal, Terminal 9 in this example. If none of the terminals (6 through 10) is available, the hunt ends and the system does not answer the call.
- Circular hunt—The incoming call is routed to the terminal with the dialed DN, Terminal 5 in this example. If Terminal 5 is busy, the system hunts for the next idle terminal, Terminal 9 in this example. If none of the terminals (6 through 10) is available, the hunt continues with Terminal 1 through 4. If none of the terminals up to n-1 (where n is the dialed DN) is available, the hunt ends and the system does not answer the call.

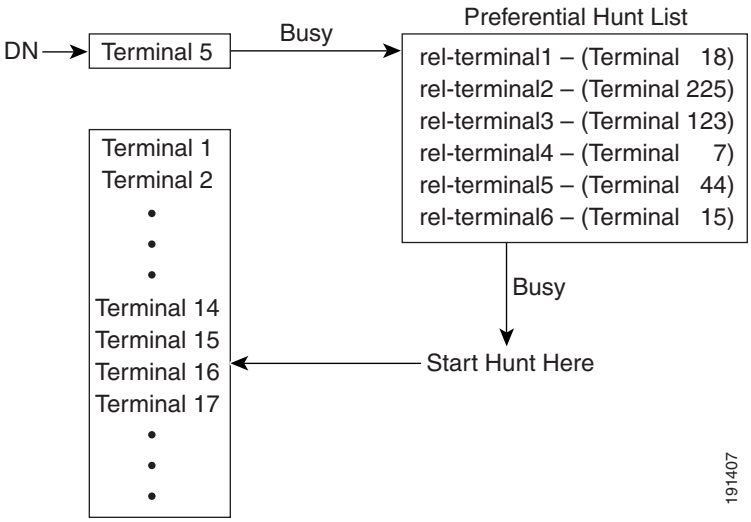
- UCD hunt—The incoming call is routed to the terminal with the dialed DN, Terminal 5 in this example. If Terminal 5 is idle, the system completes the call to Terminal 5 and does not attempt to change the NFT pointer. If Terminal 5 is busy, the system completes the call to the NFT. In this example, the system has already set the NFT pointer to Terminal 4. Therefore the call is completed to Terminal 4. When the call is completed to Terminal 4, the system performs a circular hunt for the next idle line, beginning with the terminal that follows the one on which the call was completed. It sets the NFT pointer to the next idle line (Terminal 2 in this example). The system will give the next call to Terminal 2.
- If the terminal associated with the dialed DN of the incoming call is provisioned in the Subscriber table with a mlhg-pref-list-id, the system first hunts according to the process described in the "Preferential Hunt Lists" section on page 3-93. Preferential hunting is supported only if the hunt type is regular or circular (not UCD).

Preferential Hunt Lists

The system supports preferential hunt lists. There can be up to 64 preferential hunt lists per MLHG, and a maximum of 18 terminals are allowed in each list. Preferential hunt works only if the inbound call was dialed to the DN of a specific terminal. If the called DN is busy, and if the terminal associated with that DN is provisioned in the Subscriber table with a mlhg-pref-list-id, the system first searches the preferential hunt list in a specified sequence. The call is given to the first idle member of that preferential hunt list. If all the terminals in the preferential hunt list are busy, the hunting continues in the main MLHG list starting from the terminal after the last terminal in the preferential hunt list. This process is shown in Figure 3-5.

Note The system does not invoke the preference list (preferential hunt) if hunt-type=UCD in the MLHG table.

Figure 3-5 Searching a Preferential Hunt List (Example)



MLHG Provisioning Options and Use Cases

Table 3-12 explains how provisioning in the Subscriber table affects the behavior of a terminal in the MLHG.

Table 3-12 Impact of Provisioning CATEGORY, MLHG-ID, and GRP Parameters in the Subscriber Table

Provision CATEGORY (default=INDIVIDUAL) As	MLHG-ID Required?	Provision GRP (default=N) As	Telephony Features Provided by the System and Hunt Scenario
MLHG	Required	(no effect)	This is the main subscriber for the MLHG. It is optional to assign a term-id to this subscriber.
MLHG-INDIVIDUAL or MLHG-PREF-INDIV[1]	Required	Y	The individual subscriber inherits all of the features of the main subscriber. The individual cannot be provided with any additional features. **Caution** Do not attempt to assign individual features to a subscriber when grp=y. The system will not honor these features for this subscriber. This subscriber must have a term-id that matches a term-id in the mlhg-terminal table. This terminal is included in the hunt when the pilot number is called. It can also receive calls directly to an individual DN if provisioned in the subscriber table.
MLHG-INDIVIDUAL or MLHG-PREF-INDIV	Required	N	The individual subscriber does not inherit any of the features of the main subscriber. The individual can be provided with features through regular subscriber and feature provisioning. This subscriber must have a term-id that matches a term-id in the mlhg-terminal table. This terminal is included in the hunt when the pilot number is called. It can also receive calls directly to an individual DN if provisioned in the subscriber table.
INDIVIDUAL	Not required (no effect)	(no effect)	The individual can be provided with features through regular subscriber and feature provisioning. If the term-id of this subscriber matches a term-id in the mlhg-terminal table, this line is included in the hunt when the pilot number is called. However, when the DN of this individual line is called directly, no hunting treatment is offered, even if the line is busy.

1. For individual members of the MLHG, you can provision the category parameter in the subscriber table as mlhg-individual or mlhg-pref-indiv. The system treats these settings identically.

Main subscriber—Each MLHG has a single main-sub-id, also referred to as the group ID. The main-sub-id identifies a subscriber record that contains parameters for the group, including the pilot DN. In the Subscriber table, you must assign category=mlhg (or ctxg-mlhg) to this main subscriber. Also in the Subscriber table, you can assign a term-id to this subscriber (optional).

Subscribers—Any termination reachable through an individual DN must be set up as a subscriber (provisioned with a value for DN1 in the Subscriber table), and any termination to physical line must be defined with a unique term-id (the same term-id in both the Subscriber and MLHG-Terminal tables). Any termination that can originate calls must be set up as a subscriber.

Terminals—Each line in an MLHG must have a terminal number that identifies its position in the group. You must provision a terminal number in the MLHG-Terminal table for every line in the MLHG. During a multiline hunt, the terminals are attempted in numerical order, from lowest to highest.

Features—The system delivers the same features to the subscriber regardless of how the features are assigned (assigned and activated on the individual subscriber, or inherited from the main subscriber and activated on the individual subscriber).

Feature activation—If a feature requires activation by the user, activation for one user in the MLHG does not affect activation for another user. Activation for the main subscriber does not cause activation for any of the individual subscribers, even if the subscribers have GRP=Y.

Caution For features that require activation by the user, each user has the option of activating the feature, but this does not occur automatically.

Treatment of Outbound Call Features

Temporarily disconnected status—If temporarily-disconnected status is assigned to the subscriber record for the main subscriber (Subscriber table: status=temp-disconnected), the system treats all the lines in the MLHG (that is, all the lines provisioned with the same mlhg-id as the main subscriber) as temporarily disconnected. This is true regardless of the provisioned value for the grp parameter in the Subscriber table.

Call forwarding—When a call is forwarded from a line in the MLHG, the forwarding signaling contains the DN of the subscriber associated with the original dialed number.

Account codes and authorization codes—You can provision the system to collect account codes and authorization codes from members of the MLHG. First, set up a class of service (COS) restriction in the COS-Restrict table for the appropriate account code or authorization code treatment. Then provision the subscribers as follows:

- If you want to assign the COS treatment (including account codes and authorization codes) to all members of the MLHG (that is, to all the lines provisioned with the same mlhg-id as the main subscriber), assign the COS to the main subscriber and provision all members of the MLHG with grp=Y.
- If you provision any individual subscriber with grp=N, that individual does not inherit the COS feature from the main subscriber, However, you can still provision the individual with any desired features, including any available COS.

Speed call:

- Group speed call—To provide the group speed call feature to all members of the MLHG, provision the subscriber record for every member of the MLHG with grp=Y, and provision the main subscriber with the group speed call feature (GSC1D and GSC2D).

Note When both speed call and group speed call features are assigned to the main subscriber, both the features are inherited by all members of the group (having GRP=Y in subscriber table). When a member subscriber attempts to invoke speed call feature, the individual speed calling takes precedence over group speed-calling. The group-speed-call feature is not invoked in such scenarios.

- Individual speed call—If you set grp=N for any member of the MLHG, then that member is provided only with the features assigned to the individual subscriber record (including any individual speed call features), and none of the features assigned to the main subscriber.

Treatment of Inbound Call Features

This section explains how the system treats an inbound call when a feature is assigned and active on an MLHG subscriber line. The handling of inbound calls depends on the following factors:

- The dialed directory number (DN)—This is the number dialed by the remote originating party. The dialed DN could be the pilot DN (the DN of the main subscriber of the MLHG) or the individual DN of any MLHG member.
- Active features—The treatment of the call depends on the features that are assigned and activated on the subscriber associated with the dialed DN. If a hunt occurs, the properties (the features and feature activation data) of the dialed DN are applied, not the properties of the hunted terminal.

Note If the hunted terminal goes off-hook to receive the call, the user of the hunted terminal can initiate midcall features (for example, by depressing the hook or pressing the Flash button). The midcall features are based on the properties of the individual hunted terminal.

- Call waiting tone—Call Waiting (CW) and Caller ID on Call Waiting (CIDCW) are disabled for all MLHG subscribers. The CW tone is not applied on the main subscriber or mlhg-individual endpoints under any scenario.
- Temporarily disconnected status—If temporarily-disconnected status is assigned to the subscriber record for the main subscriber (Subscriber table: status=temp-disconnected), the system does not perform any hunting, and it treats all the lines in the MLHG (that is, all the lines provisioned with the same mlhg-id as the main subscriber) as temporarily disconnected. This is true regardless of the provisioned value for the grp parameter in the Subscriber table.
- Typically, a subscriber service contains multiple features, and the system applies the features according to the normal feature precedence as documented in Chapter 5, “Feature Interactions.”

Assigning and Activating Features

This section explains what causes a feature to be assigned and active on the MLHG main subscriber and MLHG individual.

For features that require activation, individual subscribers typically activate the feature on their own handset using vertical service codes (VSCs). Activation of a feature for one member of the MLHG does not affect activation for another user. Activation for the main subscriber does not cause activation for any of the individual subscribers, even if the individual subscribers have GRP=Y.

MLHG Main Subscriber

Features are assigned directly to the main subscriber by provisioning the Subscriber Profile or Subscriber Service Profile table. For the main subscriber, a feature is active if it is assigned to the subscriber, and activated by either of the following methods:

- If a terminal is assigned to the main subscriber, the feature can be activated through handset provisioning or through the Subscriber Feature Data table.
- If a terminal is *not* assigned to the main subscriber (term=none in the Subscriber table), the feature can be activated through the Subscriber Feature Data table.

MLHG Individual

There are two methods of assigning a feature to an MLHG individual:

- Set GRP = Y in the Subscriber table—This causes the MLHG individual to inherit all the features assigned to the main subscriber.
- Set GRP = N in the Subscriber table—In this case, the MLHG individual inherits no features from the main subscriber. Individual features can be assigned directly to the individual subscriber.

Caution If you set GRP = Y for a particular MLHG individual (which causes the MLHG individual to inherit all the features from the MLHG main subscriber), do not directly add any features to the MLHG individual, This could cause unexpected feature interactions.

Table 3-13 lists the parameters that affect assignment and activation of features on the MLHG individual.

Table 3-13 Parameters Affecting Assignment and Activation of Features on MLHG Individual

Feature Assigned to Main Subscriber	MLHG Individual Subscriber			Result—Status of the Feature on the MLHG Individual	Explanation
	GRP =	Feature Assigned to MLHG Individual	Feature Activated on MLHG Individual		
Y	Y	N	Y	Active	MLHG individual inherits feature from the main sub. Feature is activated on the MLHG individual.
Y or N	N	Y	Y	Active	Feature is assigned directly to the MLHG individual. Feature is activated on the MLHG individual.
Y	Y	N	N	Not active.	MLHG individual inherits feature from the main sub. Feature is not activated on the MLHG individual.
N	Y	N	n/a	Not active.	The feature is not assigned.
Y or N	N	Y or N	N	Not active.	Regardless of feature assignment, the feature is not activated on the MLHG individual.

Treatment of Incoming Calls for Specific Features

The treatment of incoming calls is described for the features listed below.

CFB:

Table 3-14, "Treatment of Incoming Call to Pilot DN for CFB Feature"

Table 3-15, "Treatment of Incoming Call to MLHG Individual DN for CFB Feature"

CFNA:

Table 3-16, "Treatment of Incoming Call to Pilot DN for CFNA Feature"

Table 3-17, "Treatment of Incoming Call to MLHG Individual DN for CFNA Feature"

CFC or VM:

Table 3-18, "Treatment of Incoming Call to Pilot DN for CFC or VM Feature"

Table 3-19, "Treatment of Incoming Call to MLHG Individual DN for CFC or VM Feature"

CFU or VMA:

Table 3-20, "Treatment of Incoming Call to Pilot DN for CFU or VMA Feature"

Table 3-21, "Treatment of Incoming Call to MLHG Individual DN for CFU or VMA Feature"

SCA, SCF, and SCR:

Table 3-22, "Treatment of Incoming Call to Pilot DN for SCA, SCF, or SCR Feature"

Table 3-23, "Treatment of Incoming Call to MLHG Individual DN for SCA, SCF, or SCR Feature"

DRCW:

Table 3-24, "Treatment of Incoming Call to Pilot DN for DRCW Feature"

Table 3-25, "Treatment of Incoming Call to MLHG Individual DN for DRCW Feature"

CFB

Table 3-14 lists the call treatment for inbound calls to the MLHG pilot number (main subscriber DN) based on the assignment and activation of Call Forwarding Busy (CFB) for that main subscriber.

Table 3-14 Treatment of Incoming Call to Pilot DN for CFB Feature

CFB Assignment and Activation on the Main Subscriber	Scenario (Condition When Call Comes In to the Pilot DN)	Call Treatment Given to the Inbound Call
(For these scenarios, CFB assignment and activation have no effect.)	Terminal of the main-sub is busy, or no terminal is assigned to the main-sub.	The system hunts for an idle line.
	Terminal of the main-sub or hunted terminal is idle but does not answer.	Ringing on idle line.
CFB assigned and activated.	All terminals busy.	Call forwarded per CFB.
CFB assigned but not activated, or CFB not assigned.		Busy tone

Table 3-15 lists the call treatment for inbound calls to the MLHG individual subscriber DN based on the assignment and activation of CFB for that individual.

Table 3-15 Treatment of Incoming Call to MLHG Individual DN for CFB Feature

CFB Assignment and Activation on the MLHG Individual	Scenario (Condition When Call Comes In to DN of the MLHG Individual)	Call Treatment Given to the Inbound Call
(For these scenarios, CFB assignment and activation have no effect.)	Mlhg-individual is busy.	The system hunts for an idle line.
	Mlhg-individual or hunted terminal is idle but does not answer.	Ringing on idle line.

Table 3-15 Treatment of Incoming Call to MLHG Individual DN for CFB Feature (continued)

CFB Assignment and Activation on the MLHG Individual	Scenario (Condition When Call Comes In to DN of the MLHG Individual)	Call Treatment Given to the Inbound Call
CFB assigned and activated.	All terminals busy.	Call forwarded per CFB.
CFB assigned but not activated, or CFB not assigned.		Busy tone

CFNA

Table 3-16 lists the call treatment for inbound calls to the MLHG pilot number (main subscriber DN) based on the assignment and activation of Call Forwarding No Answer (CFNA) for that main subscriber.

Table 3-16 Treatment of Incoming Call to Pilot DN for CFNA Feature

CFNA Assignment and Activation on the Main Subscriber	Scenario (Condition When Call Comes In to the Pilot DN)	Call Treatment Given to the Inbound Call
(For this scenario, CFNA assignment and activation have no effect.)	Terminal of the main-sub is busy, or no terminal is assigned to the main-sub.	The system hunts for an idle line.
CFNA assigned and activated.	Terminal of the main-sub or hunted terminal is idle but does not answer.	Call forwarded per CFNA.
CFNA assigned but not activated, or feature not assigned.		Ringing on idle line.
(For this scenario, CFNA assignment and activation have no effect.)	All terminals busy.	Busy treatment.

Table 3-17 lists the call treatment for inbound calls to an MLHG individual subscriber DN based on the assignment and activation of CFNA for that individual.

Table 3-17 Treatment of Incoming Call to MLHG Individual DN for CFNA Feature

CFNA Assignment and Activation on the MLHG Individual	Scenario (Condition When Call Comes In to DN of the MLHG Individual)	Call Treatment Given to the Inbound Call
(For this scenario, CFNA assignment and activation have no effect.)	Mlhg-individual is busy.	The system hunts for an idle line.
CFNA assigned and activated.	MLHG-individual or hunted terminal is idle but does not answer.	Call forwarded per CFNA.
CFNA assigned but not activated, or feature not assigned.		Ringing on idle line.
(For this scenario, CFNA assignment and activation have no effect.)	All terminals busy.	Busy treatment.

CFC or VM

Table 3-18 lists the call treatment for inbound calls to the MLHG pilot number (main subscriber DN) based on the assignment and activation of Call Forwarding Combination (CFC) or Voice Mail (VM) for that main subscriber.

Note Information for the Voice Mail Always (VMA) feature is in Table 3-20 and Table 3-21.

Table 3-18 Treatment of Incoming Call to Pilot DN for CFC or VM Feature

Feature (CFC or VM) Assignment and Activation on the Main Subscriber	Scenario (Condition When Call Comes In to the Pilot DN)	Call Treatment Given to the Inbound Call
(For this scenario, feature assignment and activation have no effect.)	Terminal of the main-sub is busy, or no terminal is assigned to the main-sub.	The system hunts for an idle line.
Feature assigned and activated.	Terminal of the main-sub or hunted terminal is idle but does not answer.	Call forwarded per CFC or VM.
Feature assigned but not activated, or feature not assigned.		Ringing on idle line.
Feature assigned and activated.	All terminals busy.	Call forwarded per CFC or VM.
Feature assigned but not activated, or feature not assigned.		Busy treatment.

Table 3-19 lists the call treatment for inbound calls to an MLHG individual subscriber DN based on the assignment and activation of CFC or VM for that individual.

Table 3-19 Treatment of Incoming Call to MLHG Individual DN for CFC or VM Feature

Feature (CFC or VM) Assignment and Activation on the MLHG Individual	Scenario (Condition When Call Comes In to DN of the MLHG Individual)	Call Treatment Given to the Inbound Call
(For this scenario, feature assignment and activation have no effect.)	Mlhg-individual is busy.	The system hunts for an idle line.
Feature assigned and activated.	Mlhg-individual or hunted terminal is idle but does not answer.	Call forwarded per CFC or VM.
Feature assigned but not activated, or feature not assigned.		Ringing on idle line.
Feature assigned and activated.	All terminals busy.	Call forwarded per CFC or VM.
Feature assigned but not activated, or feature not assigned.		Busy treatment.

CFU or VMA

Table 3-20 lists the call treatment for inbound calls to the MLHG pilot number (main subscriber DN) based on the assignment and activation of Call Forwarding Unconditional (CFU) or Voice Mail Always (VMA) for that main subscriber.

Note Information for the Voice Mail (VM) feature is in Table 3-18 and Table 3-19.

Table 3-20 Treatment of Incoming Call to Pilot DN for CFU or VMA Feature

Feature (CFU or VMA) Assignment and Activation on the Main Subscriber	Scenario (Condition When Call Comes In to the Pilot DN)	Call Treatment Given to the Inbound Call
Feature assigned and activated.	Terminal of the main-sub is busy, or no terminal is assigned to the main-sub.	Call forwarded per CFU or VMA.
Feature assigned but not activated, or feature not assigned.		The system hunts for an idle line.
Feature assigned and activated.	Terminal of the main-sub is idle.	Call forwarded per CFU or VMA.
Feature assigned but not activated, or feature not assigned.	Terminal of the main-sub is idle but does not answer.	Ringing on idle line.
Feature assigned and activated.	All terminals busy.	Call forwarded per CFU or VMA.
Feature assigned but not activated, or feature not assigned.		Busy treatment.
Feature assigned and activated on main subscriber.	Special Case—Dialed DN of incoming call is DN of the mlhg-individual, not DN of the main-sub.	Call treatment is based on the provisioned properties (features and feature data) of the mlhg-individual.

Table 3-21 lists the call treatment for inbound calls to an MLHG individual subscriber DN based on the assignment and activation of CFU or VMA for that individual.

Table 3-21 Treatment of Incoming Call to MLHG Individual DN for CFU or VMA Feature

Feature (CFU or VMA) Assignment and Activation on the MLHG Individual	Scenario (Condition When Call Comes In to DN of the MLHG Individual)	Call Treatment Given to the Inbound Call
Feature assigned and activated.	Mlhg-individual is busy.	Call forwarded per CFU or VMA.
Feature assigned but not activated, or feature not assigned.		The system hunts for an idle line.
Feature assigned and activated.	Terminal of the mlhg-individual is idle.	Call forwarded per CFU or VMA.
Feature assigned but not activated, or feature not assigned.	Mlhg-individual or hunted line is idle but does not answer.	Ringing on idle line.
Feature assigned and activated.	All terminals busy.	Call forwarded per CFU or VMA.
Feature assigned but not activated, or feature not assigned.		Busy treatment.

SCA, SCF, and SCR

Table 3-22 lists the call treatment for inbound calls to the MLHG pilot number (main subscriber DN) based on the assignment and activation of Selective Call Acceptance (SCA), Selective Call Forwarding (SCF), or Selective Call Rejection (SCR) for that main subscriber. The system invokes the SCA, SCF, or SCR feature only if the DN of the calling party is included in the screening list of the called party.

Table 3-22 Treatment of Incoming Call to Pilot DN for SCA, SCF, or SCR Feature

Feature (SCA, SCF, or SCR) Assignment and Activation on the Main Subscriber	Scenario (Condition When Call Comes In to the Pilot DN)	Call Treatment Given to the Inbound Call
Feature assigned and activated.	Terminal of the main-sub is busy, terminal of main-sub is idle, or no terminal is assigned to the main-sub.	SCA (on list)—Hunting; see additional scenarios in this table. SCA (not on list)—Call is not accepted; SCA announcement. SCF (on list)—Call forwarded per SCF. SCF (not on list)—Hunting; see additional scenarios in this table. SCR (on list)—Call rejected per SCR with SCR announcement. SCR (not on list)—Hunting; see additional scenarios in this table.
Feature assigned but not activated, or feature not assigned.		The system hunts for an idle line.
Feature assigned and activated.	Terminal of the main-sub or hunted terminal is idle but does not answer.	SCA (on list)—Ringing on idle line. SCF (not on list)—Ringing on idle line. SCR (not on list)—Ringing on idle line.
Feature assigned but not activated, or feature not assigned.		Ringing on idle line.
Feature assigned and activated.	All terminals busy.	SCA (on list)—Busy treatment. SCF (not on list)—Busy treatment. SCR (not on list)—Busy treatment.
Feature assigned but not activated, or feature not assigned.		Busy treatment.

Table 3-23 lists the call treatment for inbound calls to an MLHG individual subscriber DN based on the assignment and activation of SCA, SCF, or SCR for that individual.

Table 3-23 Treatment of Incoming Call to MLHG Individual DN for SCA, SCF, or SCR Feature

Feature (SCA, SCF, or SCR) Assignment and Activation on the MLHG Individual	Scenario (Condition When Call Comes In to DN of the MLHG Individual)	Call Treatment Given to the Inbound Call
Feature assigned and activated.	Mlhg-individual is busy, or terminal of mlhg-individual is idle.	SCA (on list)—Hunting; see additional scenarios in this table. SCA (not on list)—Call is not accepted; SCA announcement. SCF (on list)—Call forwarded per SCF. SCF (not on list)—Hunting; see additional scenarios in this table. SCR (on list)—Call rejected per SCR with SCR announcement. SCR (not on list)—Hunting; see additional scenarios in this table.
Feature assigned but not activated, or feature not assigned.		The system hunts for an idle line.
Feature assigned and activated.	Mlhg-individual or hunted terminal is idle but does not answer.	SCA (on list)—Ringing on idle line. SCF (not on list)—Ringing on idle line. SCR (not on list)—Ringing on idle line.
Feature assigned but not activated, or feature not assigned.		Ringing on idle line.
Feature assigned and activated.	All terminals busy.	SCA (on list)—Busy treatment. SCF (not on list)—Busy treatment. SCR (not on list)—Busy treatment.
Feature assigned but not activated, or feature not assigned.		Busy treatment.

DRCW

Table 3-24 lists the call treatment for inbound calls to the MLHG pilot number (main subscriber DN) based on the assignment and activation of Distinctive Ringing Call Waiting (DRCW) for that main subscriber. The system invokes the DRCW feature only if the DN of the calling party is included in the DRCW screening list of the called party.

Note Call Waiting (CW) and Caller ID on Call Waiting (CIDCW) are disabled for all MLHG subscribers. The CW tone is not applied on the main subscriber or mlhg-individual endpoints under any scenario.

Table 3-24 Treatment of Incoming Call to Pilot DN for DRCW Feature

DRCW Assignment and Activation on the Main Subscriber	Scenario (Condition When Call Comes In to the Pilot DN)	Call Treatment Given to the Inbound Call
(For this scenario, feature assignment and activation have no effect.)	Terminal of the main-sub is busy, or no terminal is assigned to the main-sub.	The system hunts for an idle line.
Feature assigned and activated.	Terminal of the main-sub or hunted line is idle.	DRCW (on list)—Ringing per DRCW. DRCW (not on list)—Regular ringing.
Feature assigned but not activated, or feature not assigned.		Regular ringing.
(For this scenario, feature assignment and activation have no effect.)	All terminals busy	Busy treatment.

Table 3-25 lists the call treatment for inbound calls to an MLHG individual subscriber DN based on the assignment and activation of DRCW for that individual.

Table 3-25 Treatment of Incoming Call to MLHG Individual DN for DRCW Feature

DRCW Assignment and Activation on the MLHG Individual	Scenario (Condition When Call Comes In to DN of the MLHG Individual)	Call Treatment Given to the Inbound Call
(For this scenario, feature assignment and activation have no effect.)	Mlhg-individual is busy.	The system hunts for an idle line.
Feature assigned and activated.	Mlhg-individual or hunted line is idle.	DRCW (on list)—Ringing per DRCW. DRCW (not on list)—Regular ringing.
Feature assigned but not activated, or feature not assigned.		Regular ringing.
(For this scenario, feature assignment and activation have no effect.)	All terminals busy	Busy treatment.

Billing for MLHG

Billing fields for calls originated by DNs within the MLHG are populated as follows.

Field 23 (originating number):

- The value of the DN1 field of the individual subscriber, if available.
- Otherwise, the value of the DN1 field of the main subscriber.

Field 25 (charge number)

- The value of the billing-dn field of the subscriber if available.
- Otherwise, the value of the billing-dn field of the main subscriber if available.
- Otherwise, the value of the DN1 field of the main subscriber if available.
- Otherwise, the value of the DN1 field of the subscriber.

For complete billing information, see the *Cisco BTS 10200 Softswitch Billing Guide*.

Basic Provisioning Procedure and CLI Reference

For the basic sequence of steps to provision a MLHG, see the MLHG provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

To see a detailed list of all provisionable values for the MLHG, MLHG Terminal, and MLHG Preference List tables, see the applicable tables in the *Cisco BTS 10200 Softswitch CLI Database*.

Multiline Variety Package

The MVP feature allows the creation of a logical grouping of subscribers and enables the provision of Centrex features such as call-hold, call-park/retrieve and extension dialing for the subscribers within the group.

Typically Centrex subscribers dial “9” (or some other access code) to access the public switched telephone network (PSTN) and dial extension numbers to reach other subscribers within the group. However, in the case of small businesses with fewer lines, it can be expected that most of the originating call traffic will be towards the PSTN and not within the group.

Using the MVP feature on the BTS 10200 system (as explained in the provisioning steps described in next section), the requirement to dial an access code to access a PSTN line can be avoided for the group members.

In addition, the BTS10200 can be configured to use “*” prefixed extensions to reach the subscribers within the group. It is possible to use 1-digit extensions within the range *2–*9 for a smaller group of subscribers (that is, a group with up to 8 subscribers) or 2-digit extensions within range *20–*49 for a medium size group of subscribers (that is, a group with up to 30 subscribers). *0 can be assigned to the operator or *0 can be used for Operator or Attendant Access.

Provisioning Procedure

For information on the provisioning procedure for the MVP feature, refer to *Cisco BTS 10200 Softswitch Provisioning Guide*.

Multiple Directory Numbers (MDN)

Multiple directory numbers (MDN) service is also known as teen service. It enables one primary DN and multiple secondary DNs to be assigned to a single line termination. A specific unique ringing pattern is assigned to each DN, so that each incoming call can be individually identified. A distinctive CW tone is also assigned to each DN so that each incoming call can be individually identified when the line is busy.

Billing for this service is charged to the primary telephone number (or to the number designated as the billing DN). If DRCW is activated, MDN is inhibited. For calls originating from a MDN line, the primary DN is used as caller-ID, if an ID is offered to the called party.

Note The MDN feature is available to POTS users only.

Tip To provision this feature, see the MDN provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

No Solicitation Announcement (NSA)

The NSA feature allows subscribers to play a message telling callers that they do not accept solicitation (telemarketing) calls. The feature does not forcibly release the call, but the expectation is that any solicitation caller will hang up. The subscriber can manage a number of NSA parameters via the handset, including activation/deactivation of the feature, time-of-day activation options, a list of directory numbers (DNs) for which the announcement will be bypassed, and a private identification number (PIN) for access to management options.

During the setup process for the incoming call, if the NSA feature has been assigned by the service provider and the called party (subscriber) has the feature activated, the NSA announcement is played to the caller. (However, the announcement is bypassed if the subscriber has included the DN of the incoming caller on their NSA bypass list.) The announcement also notifies the caller to press a specific key on the handset (default is **1**) to bypass the announcement and connect to the subscriber. If the caller waits until the announcement completes, the call is connected to the subscriber.

The NSA feature requires support from an interactive voice response (IVR) server in the network, and from the BTS 10200 screening list editing (SLE) feature. The BTS 10200 establishes a Real-Time Transport Protocol (RTP) connection between the incoming media gateway (MGW) or integrated access device (IAD) and the IVR server.

Tip For more details about the IVR interactions for this feature, see Chapter 6, "Interactive Voice Response Functions."

References

The following standards are available:

- PacketCable document PKT-SP-ASP-I02-010620, *PacketCable Audio Server Protocol Specification*
- PacketCable document PKT-TR-VOIPERF-R01-000831, *Extended Residential Feature Descriptions for PacketCable-Based VOIP Services*, Section 2.1.9 (No Solicitation Announcement)
- Telcordia document GR-220-CORE, *Screening List Editing*

NSA Activation, Management, and Control

The service provider assigns the NSA feature to subscribers. The feature is in the deactivated mode when assigned, unless activated by the service provider or subscriber.

Note The system allows the service provider to provision these features for the subscriber, but typically these features are provisioned from the subscriber handset via a connection to an IVR server.

The feature supports the following management and control procedures for the subscriber:

- Establish a pass code (required to access the management menu):

  The subscriber must enter a PIN for authentication purposes when accessing the IVR system to change the NSA settings. The subscriber is allowed to choose the PIN when the service provider initially assigns the feature. After that, the subscriber cannot change the PIN unless the service provider resets it. The service provider can enable (or disable) the PIN authentication step by setting the AUTH-ENABLED token to Y (or N) in the Feature Configuration (feature-config) table. The default value is Y.

- Create and edit a list of directory numbers (DNs) for bypassing the NSA announcement:

  The subscriber can provision a list of calling DNs that are allowed to bypass the NSA announcement and go directly to the subscriber line. The list can contain full DNs, partial DNs, and extension numbers (if the subscriber is in a Centrex group). By default, the system allows subscribers to program up to 31 DNs in the NSA bypass list. The service provider can reset the limit of DNs to any number from 2 to 31 by tuning the value of the SLE-LIST-SIZE token in the Call Agent Configuration (ca-config) table.

  For each DN entry, the system accepts up to 16 digits (and ignores any additional digits entered by the handset user). The system checks that the digit string represents a valid calling number before storing it in the database. If the digit string does not represent a valid calling number, the system plays a denial announcement to the handset user.

  - When DN-TYPE=FDN, the system normalizes the number before storing it in the database. Normalization means that the system performs the digit manipulation provisioned in the Digit Manipulation (digman) table. For example, if a user enters 19725551212, the digman table might normalize to 9725551212.
  - The system allows DN-TYPE=EXTENSION only if the subscriber line is a Centrex line. The system checks that the digit string entered by the handset user is a valid extension for the local Centrex group.
  - When DN-TYPE=PARTIAL, the system accepts any digit string up to 16 digits.

Tip To activate the NSA service, the subscriber must enter at least one DN on the NSA bypass list. This is consistent with the requirements of GR-220. If the subscriber would like to play the NSA announcement to every caller, the subscriber must enter one DN, which should be a number that is generally not used (for example, 555-555-5555).

- Specify the schedule (time slots) when NSA service will be active:

  This setting allows the subscriber or the service provider to set the time slots when the NSA service will be active. The provisioning by the service provider can be at the office level or the subscriber level. The values provisioned by or for the subscriber take precedence over the values provisioned

at the office level. The subscriber may provision the time slots (days of the week and time of day) when the service will be active. At all times other than the provisioned time slots, the service is deactivated. During NSA nonservice hours, the following apply:

- There is no announcement, and calls go directly to the subscriber line.
- The NSA bypass list and other settings for the subscriber are preserved.

The service provider can enable or disable the handset-based schedule management via options in the feature-config table.

- Toggle a parameter to turn NSA on or off.

Tip For information on the feature-config and ca-config tables, seethe *Cisco BTS 10200 Softswitch CLI Database*, and use the **show feature-config** and **show ca-config** commands.

NSA Invocation

NSA invocation refers to the implementation of the NSA feature by the system during call setup. The NSA feature works in conjunction with the network IVR server to prompt the caller and control the invocation process.

For callers calling an NSA subscriber during the time period configured as active by the subscriber, and not on the subscriber's NSA bypass list, the NSA feature plays an announcement similar to "You have reached a number that does not accept phone solicitations. If you are a solicitor, please add this number to your do-not-call list and hang up now. Otherwise, please press **1**, or stay on the line." The caller may then take any of the following actions:

- Stay on the line, or press 1—In this case, the subscriber is rung and the call is connected to the subscriber.
- Hang up—In this case, the system does not ring the subscriber.
- Press a digit other than 1—In this case, the NSA announcement is replayed to the caller. When the number of replay attempts exceeds a provisioned threshold, the subscriber will be rung and the caller will be connected to the subscriber.

Feature Interactions

Feature interactions are as follows:

- NSA and Anonymous Call Rejection (ACR):
  If the subscriber gets an anonymous call and has both NSA and ACR features active, the incoming call is given the ACR feature. ACR has a higher priority than NSA even for anonymous callers who are on the NSA priority caller list.
- NSA and Privacy Screening (PS):
  If the subscriber receives an anonymous call and has both PS and NSA features active, the subscriber is given the PS feature. For nonanonymous callers, the subscriber is given the NSA feature.
- NSA and Selective Call Rejection (SCR):
  If a subscriber receives a call from a caller whose DN is in the SCR list for the subscriber, the caller hears the SCR announcement and is blocked by SCR. If the subscriber is not on the SCR list, the subscriber is given the NSA announcement.

- NSA and Call Forwarding Unconditional (CFU):
  If the subscriber has CFU and NSA active, an incoming call is given the NSA feature. If the caller chooses to continue with the call and if the subscriber has CFU active, the call will be forwarded by CFU.
- NSA and VM:
  If the subscriber has VM and NSA active, an incoming call will be given the NSA feature. If the caller chooses to continue with the call and if the subscriber has VM active, the call will be forwarded by VM.
- NSA and Call Forwarding Busy (CFB):
  If the subscriber has both NSA and CFB active, the caller will first hear the NSA announcement. If the caller chooses to continue with the call and if the subscriber is busy and has CFB active, the call will be forwarded by CFB.
- NSA and Call Forwarding No Answer (CFNA):
  If the subscriber has both NSA and CFNA active, the caller will first hear the NSA announcement. If the caller chooses to continue with the call and if the subscriber does not answer and has CFNA active, the call will be forwarded by CFNA.
- NSA and Do Not Disturb (DND):
  If the subscriber has both NSA and DND assigned and active, the caller will be rejected by DND.
- NSA and Selective Call Acceptance (SCA):
  If the subscriber receives an anonymous call from a caller whose DN is not in the SCA list for the subscriber, the call will be blocked by SCA.
- NSA and Selective Call Forwarding (SCF):
  If the subscriber receives a call from a caller whose DN is in the SCF list for the subscriber, the call will be forwarded by SCF.
- NSA and Distinctive Ringing/Call Waiting (DRCW):
  If the subscriber receives a call from a caller whose DN is in the DRCW list for the subscriber, the call will be completed by DRCW.
- NSA and Busy Line Verification (BLV):
  If the subscriber has both NSA and BLV assigned and active, when BLV is invoked, NSA is inhibited.

Note Several of the items below use the term hookflash. In this document, hookflash means to press the Flash button (on phones that have a Flash button) or depress the hookswitch. This is the action that a subscriber typically performs to invoke a multiparty feature in the middle of a call.

- NSA_ACT and Call Waiting (CW):
  NSA Activation (NSA_ACT) does not interact with CW. The subscriber can be subscribed to both features, but may not use them simultaneously. When a subscriber is accessing NSA_ACT, CW tones are inhibited, and if the subscriber hookflashes, this ends the NSA_ACT session.
- NSA and Call Waiting (CW):
  If the subscriber is busy and does not have the CW feature, the caller will hear the NSA announcement before hearing the busy tone.
- NSA_ACT and Hookflash:
  Hookflash during a NSA_ACT session will cause the NSA activation session to end. The hookflash moves the caller back to the original call and reconnects to the held party. If the customer is subscribed to one of the multiple-party features (for example, TWC, CT, or CHD), the call is simply reconnected.

- NSA and Hookflash:
  If Subscriber A is on a call, then hookflashes and calls an NSA Subscriber B, receives the NSA announcement from Subscriber B, then Subscriber A hookflashes again during the NSA announcement, the following behaviors apply:
  - If Subscriber A and Subscriber B are on the same BTS 10200, the system ignores the second hookflash by Subscriber A, and the NSA treatment continues.
  - If Subscriber A is on a BTS 10200 and Subscriber B is on different switch, the system honors the second hookflash by Subscriber A.

Note If Subscriber B is on a different switch, the BTS 10200 honors the second hookflash because it assumes the call has been answered by Subscriber B.

Note See Chapter 5, "Feature Interactions," for a complete list of feature interactions.

Prerequisites

This feature requires connection to a network media server with IVR capabilities. The media server must support the Media Gateway Control Protocol (MGCP) basic audio (BAU) package. A voice path must be set up between the subscriber (who is using the handset) and the IVR server to allow the subscriber to activate and manage the NSA feature.

The process of creating and editing the NSA bypass list on the IVR server requires that the screening list editing (SLE) feature be provisioned on the BTS 10200. The SLE provisioning information is included in this document.

Note The SLE feature used with NSA is provisioned separately from the SLE feature used with the BTS 10200 SCA, SCF, SCR, and DRCW features. However, to the subscriber, the IVR handset operations are very similar.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the NSA provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Own Calling Number Announcement (OCNA)

The OCNA feature enables the BTS 10200 to play an announcement with the calling number when a specific pilot number is dialed. The announcement is simply the dialed digits of the calling number, and the announcement is played if the calling party is a subscriber. Calls originating outside the system are released with cause code CA_CCITT_NE_CAUSE_UNALLOCATED_NUM.

For Multiline Hunt Group (MLHG) and Centrex subscribers (INDIVIDUAL, MLHG_INDIVIDUAL, and CTXG_INDIVIDUAL), the announcement heard is the number from the directory number (DN)1 field of the Subscriber table. For all other types of subscribers, the announcement played is the calling number, if available.

The applicable cause code is 1306, OWN_CALLING_NUM. The Cisco Announcement Server ID is 903, and the ThinkEngine Networks Announcement Server ID is 92.

In Release 5.0, MR1, the handset user can activate the feature through a vertical service code (VSC). You can continue to activate the OCNA feature by provisioning a dial plan and destination.

The following limitations apply:

- The OCNA is only played if the calling party is a subscriber. Non-subscriber calls are released with cause code CA_CCITT_NE_CAUSE_UNALLOCATED_NUM.
- The OCNA feature is used during line installation/turn-up. The feature invocation occurs when a DN is not already involved in a call and will not be provided if attempted after a hookflash from a DN already involved in a call.

Tip To provision this feature, see the OCNA provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

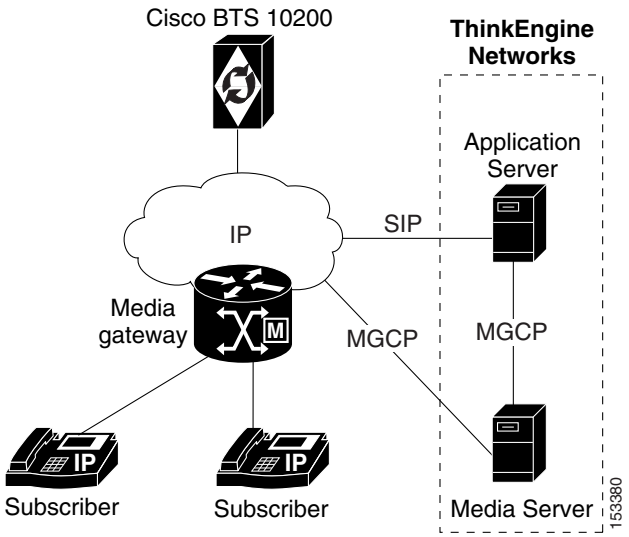
Privacy Screening (Calling Identity with Enhanced Screening)

The Privacy Screening feature enables a subscriber to accept or reject an anonymous call based on a short message recorded by the caller. This feature allows the caller to:

- Record a short message—After listening to the message, the subscriber can accept or reject the incoming call or forward it to voice mail.
- Enter a private identification number (PIN)—Entering the correct PIN rings the subscriber, and the call becomes a regular call.

Privacy Screening works in conjunction with a ThinkEngine Networks Privacy Screening Application Server (AS) and Media Server (MS) capable of interactive voice response (IVR functionality), as shown in Figure 3-6.

Figure 3-6 Example of Privacy Screening Configuration



Tip For more details about the IVR interactions for this feature, see Chapter 6, "Interactive Voice Response Functions."

Privacy Screening Description

The Privacy Screening feature is composed of the following two subfeatures:

- Privacy Screening Invocation
- Privacy Screening Subscriber Management

Privacy Screening Invocation

The Privacy Screening feature is implemented when the BTS 10200 reroutes an incoming anonymous call to the Application Server (AS) via a SIP trunk. The Cisco BTS 10200 Softswitch handles call processing for the call to the AS and for the call from the AS to the subscriber. The AS accepts the incoming call and performs the remaining functions, for example, connecting to the Media Server (MS), collecting the PIN, and recording the message.

The AS determines the active/inactive status of the Privacy Screening feature. All anonymous calls to a Privacy Screening subscriber will terminate on the AS even when the feature is inactive for the subscriber. If the Privacy Screening feature is inactive, the AS forwards the call to the subscriber.

Note If the AS is not reachable, incoming anonymous calls for the subscriber will be terminated on the subscriber.

The Privacy Screening feature is invoked using the following steps:

1. Caller A places an anonymous call to Subscriber B. Subscriber B has activated the Privacy Screening feature.
2. The call is intercepted by the Privacy Screening feature, which plays an announcement asking Caller A to either enter a PIN or wait to record a short message to be delivered to Subscriber B.

3. If Caller A enters the correct PIN, the call is forwarded to Subscriber B and becomes a regular call from this point forward. If Caller A enters an incorrect PIN, they are prompted to reenter the PIN for a maximum number of times.
4. If Caller A waits, they hear an announcement asking then to record a short message, usually their name.
5. Caller A records the message and is placed on hold.
6. A call is placed to Subscriber B to play the recorded message. Subscriber B has the following choices:
   - Review the caller name
   - Accept the call
   - Forward the call to voice mail, if the user subscribes to the voice mail feature
   - Play the not available announcement
   - Play the no solicitation announcement
   - Replay this menu
7. The call is connected or disconnected according to the choice made by Subscriber B.

Privacy Screening Subscriber Management

The BTS 10200 determines if the subscriber is subscribed to the Privacy Screening feature and, if so, reroutes the call to the AS. The AS accepts the incoming call from the subscriber and performs management functions, including collecting the PIN, changing the PIN, and changing the active/inactive status.

Synchronization of Privacy Screening Status

The BTS 10200 processes Privacy Screening feature status updates, regardless of whether the feature is active or inactive due to star code or Digital Voice Portal processing on the AS.

If Privacy Screening is deactivated, the BTS 10200 does not relay the call to the Privacy Screening AS, and it invokes other features in the feature sequence.

If the Privacy Screening feature status is activated, the BTS 10200 relays the call to the ThinkEngine Networks AS for Privacy Screening handling.

Feature Interactions

This section describes the interaction of other subscriber features with the Privacy Screening feature.

Privacy Screening and ACR

If a subscriber has the Privacy Screening feature, calls will not receive the Anonymous Call Rejection (ACR) treatment, even if Privacy Screening is inactive. Privacy Screening and ACR are mutually exclusive features.

Privacy Screening and NSA

If a subscriber has both the Privacy Screening and No Solicitation Announcement (NSA) features assigned and active and receives an anonymous call, the Privacy Screening feature will be activated. If they receive a nonanonymous call, the NSA feature will be activated.

Privacy Screening and Caller-ID

On a call received by the subscriber from the AS, “PRIVACY SCREENING” or the AS directory number (DN) will be displayed.

Privacy Screening and Distinctive Ringing

A distinctive ringing tone is played for calls received by the subscriber.

Privacy Screening and CW/CIDCW/CWD

If a subscriber is on a call and receives a call placed by the Privacy Screening AS, the subscriber receives a distinctive call waiting tone. If the subscriber has the CIDCW feature active, the caller ID will display “PRIVACY SCREENING” or the AS DN.

Privacy Screening and Voice Mail

- If a subscriber has Voice Mail Always (VMA) active, Privacy Screening calls will be forwarded to voice mail.
- If the subscriber is busy on another call or does not answer and has VM active, a Privacy Screening call will be forwarded to voice mail.

Privacy Screening and CFU/CFB/CFNA

- If a subscriber has Call Forwarding Unconditional (CFU) active, an incoming anonymous call will receive Privacy Screening and, if the caller records his or her name or enters a correct PIN, CFU forwards the call to the forward-to DN.
- If the forwarded-to number is busy and the subscriber has Call Forwarding Busy (CFB) active, CFB forwards the call to the forward-to DN.
- If the subscriber has Call Forwarding No Answer (CFNA) active and does not answer, CFNA forwards the call to the forward-to DN.

Privacy Screening and DND

If a subscriber has both Privacy Screening and Do Not Disturb (DND) assigned and activated, an incoming anonymous call is assigned to the DND feature.

Privacy Screening and SCR

If a subscriber receives an anonymous call from a caller whose DN is in the subscriber’s Selective Call Rejection (SCR) list, SCR blocks the call. If the caller’s DN is not in the SCR list and the subscriber has Privacy Screening activated, the call receives Privacy Screening.

Privacy Screening and SCA

If a subscriber receives an anonymous call from a caller whose DN is not in the Selective Call Acceptance (SCA) list, SCA blocks the call. If the caller's DN is in the SCA list and the subscriber has Privacy Screening active, the call receives Privacy Screening.

Feature Precedence

If a subscriber has Privacy Screening and DND features active, the following precedence chain will be implemented:

SCR>SCA>SCF>DRCW>Privacy Screening>ACR>CFU>DND>NSA

Feature Provisioning Commands

Tip To provision this feature, see the Privacy Screening provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Speed Call

The speed call feature is based on LSSGR module FSD 01-02-1101 (TR-TSY-000570), *Speed Calling.*

Speed Call for Individual Subscribers

The speed call feature allows a user to program the phone line so that they can dial selected or frequently called numbers using just one or two digits. After programming the line from their handset, the user can enter the one- or two-digit number, followed by the # symbol or a four-second delay, and the system automatically dials the applicable DN. The programming data is stored in the SC1D (one-digit) or SC2D (two-digit) table of the Cisco BTS 10200 Softswitch. These tables can also be programmed by the service provider via CLI commands.

To program the line, the user listens for a dial tone, then enters the VSC for one-digit or two-digit speed dial. VSCs are provisionable by the service provider. The VSCs listed below are examples:

- *74 is used for one-digit speed call, which accommodates up to 8 numbers (2 through 9)
- *75 is used for two-digit speed call, which accommodates up to 30 numbers (20 through 49)

After entering the service code, the user can either enter the end-of-dialing signal (#) or wait 4 seconds to receive the recall dial tone (stutter tone). After receiving recall dial tone, the user enters the appropriate one-digit or two-digit speed code followed by the complete phone number (including any prefixes such as 1 and the area code). A confirmation tone is then returned to the user, followed by a delay of one to 2 seconds, and then regular dial tone. Changes to existing programmed speed codes are also made in the manner described above.

After the speed code is programmed, the user can speed call as follows:

1. Go off hook and enter the one- or two-digit speed code instead of the phone number.
2. Press the # symbol or wait for 4 seconds.
3. The system automatically places the call to the DN associated with the speed code.

Tip To provision this feature, see the Speed Call provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Group Speed Call

The group speed call feature allows members of a Centrex group or multiline hunt group (MLHG) to program a list so that they can select and dial frequently called numbers using one or two digits. The group speed call provisioning process is similar to provisioning for individual subscribers, but also involves provisioning of the custom dial plan table. A handset user is allowed both one- and two-digit speed calling. In the case of shared lists for group speed calling, only one of the users sharing the list can have the user-changeable option. The switch is able to provide a given line with both a shared list and an individual list with the requirement that one must be a one-digit list and the other a two-digit list.

If speed calling is assigned to a multiline hunt group, all members of that group have access to the shared group speed call list. If, however, a line in the group also has individual speed calling, then the individual speed calling takes precedence over the group speed calling.

Note When both speed call and group speed call features are assigned to the main subscriber, both features are inherited by all members of the group (having GRP=Y in subscriber table). When a member subscriber attempts to invoke speed call feature, the individual speed calling takes precedence over group speed-calling. The group-speed-call feature is not invoked in such scenarios.

Tip To provision this feature, see the Group Speed Call provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Subscriber-Controlled Services and Screening List Editing (SLE)

Subscriber-controlled services allow individual users to screen and manage their incoming calls. The user can specify lists of DNs for which incoming calls are to be screened and given any of the following treatments—Selective Call Forwarding (SCF), Selective Call Acceptance (SCA), Selective Call Rejection (SCR), and Distinctive Ringing/Call Waiting (DRCW). The user can create screening lists, add DNs to the lists, and edit the lists, via the screening list editing (SLE) function as described in the Telcordia document *GR-220-CORE, Screening List Editing.*

CORBA Interface

The Cisco BTS 10200 Softswitch provides the necessary CORBA interface for service providers interested in building web-based applications that permit users to perform these SLE functions via the web. A web CORBA software development kit (SDK) is provided as part of the Cisco BTS 10200 Softswitch product.

User Access

The user accesses the SLE functions, including activation/deactivation of the services, via VSCs. Each VSC connects the user to the appropriate interactive voice response (IVR) media server functions. The VSCs are preprovisioned in the Cisco BTS 10200 Softswitch as listed below.

Note For each feature, a pair of preprovisioned VSCs is listed. Either VSC in the pair can be used to access the IVR server to perform all review, edit, activation, and deactivation functions. The service provider has the option of reprovisioning VSCs as desired.

- Selective Call Forwarding (SCF)—*63/*83
- Selective Call Acceptance (SCA)—*64/*84
- Selective Call Rejection (SCR)—*60/*80
- Distinctive Ringing/Call Waiting (DRCW)—*61/*81

The individual features are described in the sections that follow.

Tip For more details about the IVR interactions for this feature, see Chapter 6, "Interactive Voice Response Functions."

Tip To provision these features, see the Screening List Editing (SCF, SCA, SCR, DRCW) provisioning procedures in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Selective Call Forwarding (SCF)

The selective call forwarding (SCF) feature screens each incoming call to determine whether the DN is on a list of DNs, provisioned by the user (called party), to receive automatic forwarding treatment. The user also sets the forward-to number. Any incoming calls from DNs that are on the SCF screening list are forwarded to the designated number. Any incoming calls from DNs not on the SCF screening list receive regular treatment (they are not forwarded).

Note The service provider can provision a reminder ring for the SCF feature. For a description of reminder ring, see the "CFU Activation (CFUA)" section on page 3-8.

The user accesses and controls the SCF properties from their handset via a VSC and IVR interaction. The user can add or delete DNs on the screening list, change the forward-to number, review the screening list, and activate or deactivate SCF. As a convenience, the system allows the user to add or delete the last caller's number to the screening list by entering **01** at the prompt. The system recognizes the "01" command and translates it into the last-received DN.

The following conditions apply to the use of the SCF feature:

- TWC and CW are disabled while the user is editing the list or activating/deactivating the SCF feature.
- If SCF is active, it takes precedence over all other call forwarding features including CW and DRCW. It does not take precedence over SCR.
- The forward-to number defined in SCF can be the same number used by other call forwarding features, or it can be different.
- Once the SCF feature is activated, it remains active until it is deactivated.

Selective Call Acceptance (SCA)

The selective call acceptance (SCA) feature screens each incoming call to determine whether the DN is on a list of DNs, provisioned by the user (called party), to be accepted. Any incoming calls from DNs on the SCA screening list are accepted, but any incoming calls from DNs not on the SCA screening list are blocked (receive terminating treatment).

The user accesses and controls the SCA properties from their handset via a VSC and IVR interaction. The user can add or delete DNs on the screening list, review the screening list, and activate or deactivate SCA. As a convenience, the system allows the user to add or delete the last caller's number to the screening list by entering **01** at the prompt. The system recognizes the 01 command and translates it into the last-received DN.

The following conditions apply to the use of the SCA feature:

- TWC and CW are disabled while the user is editing the list or activating/deactivating the SCA feature.
- Once the SCA feature is activated, it remains active until it is deactivated.

Selective Call Rejection (SCR)

The selective call rejection (SCR) feature screens each incoming call to determine whether the DN is on a list of DNs, provisioned by the user (called party), to be blocked. The blocked caller is connected to an announcement stating that their call is not presently being accepted by the called party. Any incoming calls from DNs not on the SCR screening list receive regular treatment (they are not blocked).

The user accesses and controls the SCR properties from their handset via a VSC and IVR interaction. The user can add or delete DNs on the screening list, review the screening list, and activate or deactivate SCR. As a convenience, the system allows the user to add or delete the last caller's number to the screening list by entering **01** at the prompt. The system recognizes the 01 command and translates it into the last-received DN.

The following conditions apply to the use of the SCR feature:

- TWC and CW are disabled while the user is editing the list or activating/deactivating the SCR feature.
- If SCR is active, it takes precedence over all call forwarding features including CW and DRCW.
- Once the SCR feature is activated, it remains active until it is deactivated.

Note The call block/reject caller feature (see "Call Block - Reject Caller (CBLK)" section on page 3-78) provides another way for the user to selectively reject calls from the last caller.

Distinctive Ringing/Call Waiting (DRCW)

The distinctive ringing/call waiting (DRCW) feature screens each incoming call to determine whether the DN is on a list of DNs, provisioned by the user (called party), to receive special ringing or CW alerting treatment. If the incoming DN is on the DRCW screening list, the system alerts the user with a special ring or a special CW tone. Any incoming calls from DNs not on the DRCW screening list receive regular treatment (regular ringing and CW alerting tones).

The user accesses and controls the DRCW properties from their handset via a VSC and IVR interaction. The user can add or delete DNs on the screening list, review the screening list, and activate or deactivate DRCW. As a convenience, the system allows the user to add or delete the last caller's number to the screening list by entering **01** at the prompt. The system recognizes the 01 command and translates it into the last-received DN.

Once the DRCW feature is activated, it remains active until it is deactivated.

Note The DRCW feature is only for playing a distinctive ringing or distinctive call-waiting tone, and does not affect the activation of the call-waiting features (CW, CWD, or CIDCW). A subscriber must have CW, CWD, or CIDCW provisioned and activated in order to receive call-waiting treatment.

Temporarily Disconnected Subscriber Status and Soft Dial Tone

This feature allows the service provider to assign a status of temporarily disconnected (TDISC) to specific subscribers, and restrict incoming and outgoing calls for those subscribers. Using this feature, the service provider can block subscribers with delinquent accounts from making any outbound calls to numbers other than (for example) emergency, repair services, or billing department. Incoming calls disconnected due to TDISC hear an appropriate generic announcement.

This feature is applicable to POTS and Centrex subscribers. For Centrex applications, the service provider can provision the TDISC feature at the individual subscriber level and at the main-subscriber level.

Note The system never attempts to perform COS screening on call types EMG (including 911), EXTENSION, or VSC. There is no provisioning option to allow COS screening to occur on these call types.

Provisioning Options and System Behavior

This section describes the system behavior for subscribers in the TDISC state, which is dependent on certain parameters provisioned in the database.

- Scenario 1, total service denial—This option prohibits all calls, both incoming and outgoing. No dial tone and no emergency service are available for a subscriber in this state. To set this option (total service denial), provision STATUS=TEMP-DISCONNECTED in the subscriber table, and TEMP-DISC-SERVICE-ALLOWED=N in the pop table.

Note The system checks the value of the TEMP-DISC-SERVICE-ALLOWED token in the main-subscriber pop table only if the STATUS token in the subscriber table is set to TEMP-DISCONNECTED.

- Scenario 2, limited service (soft dial tone)—This option prohibits all calls, both incoming and outgoing, except for calls to/from emergency services (for example, 911) and other specific DNs, such as repair (611) or other numbers configured by the service provider. To set this option, provision as follows:
  - Provision STATUS=TEMP-DISCONNECTED in the subscriber table.

- Provision TEMP-DISC-SERVICE-ALLOWED=Y in the main-subscriber pop table. This setting causes the system to provide only those services consistent with the provisioning of the COS restrictions identified in the TEMP-DISC-COS-RESTRICT-ID token in the pop table.
- Provision TEMP-DISC-COS-RESTRICT-ID=<ID of the applicable cos-restrict table> in the pop table. The system screens calls dialed by the TDISC subscriber according to this cos-restrict table.
- Provision the applicable cos-restrict table to provide only the intended services, for example, emergency (such as 911), repair, and billing. This process may also include provisioning other tables such as the nod-wb-list table.

Note In the POP table, TEMP-DISC-COS-RESTRICT-ID is a mandatory field if TEMP-DISC-SERVICE-ALLOWED is set to Y. The value provisioned for TEMP-DISC-COS-RESTRICT-ID must match the ID of a valid COS-RESTRICT table, otherwise the system will not allow the command to go through.

- Provision TEMP-DISC-ROUTE and CUSTOMER-SUPPORT-DN in the main-subscriber POP table to provide the desired treatment to the call.

Tip You can provision the trigger-nod-escape-list table to exclude specific call types from sending triggers at specific trigger ID points in the call. COS screening (at the COS-TRIGGER point in the call) can be bypassed for specific call types if provisioned appropriately in this table.

Feature Interactions

The following features interactions occur when the subscriber is in TDISC status.

Interaction of TDISC and BLV

The system does not allow busy line verification (BLV) on lines that are in TDISC status. A BLV attempt returns the same tone to the Operator as for the “BLV line not allowed” condition.

Interaction of TDISC and MIDCALL Features

All hookflash features (MIDCALL features) are blocked for a subscriber in TDISC status. Therefore, these users cannot initiate third-party calls. If the TDISC user wants to dial a call (even if it is an emergency/911 call) while on a basic call, the user will have to hang-up the basic call and then dial the next number separately.

Interaction of TDISC and VSC-Activated Features

The vertical service code (VSC) capability is blocked for a TDISC subscriber. Features such as the customer originated trace (COT) will not work for a subscriber in TDISC status.

Restrictions and Limitations

The following restrictions and limitations apply to the TDISC feature:

- A subscriber trying to reach a TDISC subscriber normally hears an announcement that the terminating side is temporarily disconnected. However this announcement cannot be played if the terminating side is an ISDN subscriber and the route to reach that subscriber was anything other than subscriber routing in the Cisco BTS 10200 Softswitch. The routing used to reach the terminating subscriber's DN1 under these conditions must be subscriber routing.
- Trunk-grp routing for TDISC is not supported.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the Temporary Disconnect provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Three-Way Calling (TWC)

The Cisco BTS 10200 Softswitch supports the three-way calling (TWC) feature as specified in LSSGR module FSD 01-02-1301 (TR-TSY-000577), *Three-Way Calling*.

Limitations

If your network uses an ISUP variant other than ANSI ISUP, the system supports TWCD, but not TWC or USTWC.

Feature Description

TWC is a feature provisioned by the service provider in response to a request from the subscriber. TWC allows a subscriber to add a third party to an existing two party conversation.

To activate a TWC, a user involved in a stable two-way call takes the following steps:

- The user presses the **Flash** button or **hookswitch**. This places the remote end on hold.
- The user hears the recall dial tone (three tones and then a dial tone), indicating the system is ready to receive the DN for the third party.
- The user dials the DN of the third party.

Note If the user presses the **Flash** button or **hookswitch** before completing dialing, the original two-way connection is reestablished.

- When the third party answers, only the user (who initiated the TWC) and the third party can hear and talk. This allows the user to speak privately with the third party before sending the second flash.
- If the user presses the **Flash** button or **hookswitch** after successfully dialing the third party number, a three-way conference is established.

- If either of the called parties (the two stations remote from the initiating party) hangs up, the call continues as a single-call session.
- When in a TWC, the last party added can be disconnected by using the **Flash** button or **hookswitch**.
- If the initiating party hangs up during a TWC, all parties are disconnected, unless the initiating party is also subscribed to CT (see the "TWC Feature Interactions" section on page 3-122).

Note During a TWC, the CW feature does not work for the party that initiated the TWC, but does work for the two called parties.

TWC Feature Interactions

When the TWC-initiating party hangs up during a TWC, and the TWC-initiating party is not subscribed to call transfer (CT), all parties are disconnected.

However, if the TWC-initiating party is also subscribed to CT (as provisioned in the subscriber-feature-profile table), the two remaining parties stay connected. The following scenarios occur, depending upon the actions of the parties in the call. In these scenarios, User A is subscribed to both CT and TWC and is the TWC-initiating party, B is the party in the initial established call with A, and C is the third party:

- User A is in a stable call with B, places B on hold and dials C.
- If A hangs up after successfully dialing C (C is ringing), a two-way call is established between B and C, regardless of whether C answers the call. User A is billed for a call transfer, but is not billed for the time that the other two parties are on the call.
- If A waits until C answers the call, and then A hangs up, a two-way call is established between B and C. User A is billed for a call transfer and is also billed for the entire duration starting from the time A initiated the TWC until B and C hang up.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the TWC provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Three-Way Calling Deluxe (TWCD)

TWCD allows a user to add a third party to an existing two party conversation without operator assistance. The user subscribed to TWCD can use this feature regardless of which party originated the two-party call. The following conditions apply to the TWCD feature:

- The TWCD feature can be provided to POTS, Centrex, and MLHG subscribers.
- The TWCD feature is activated by the service provider at the request of the subscriber, and remains active unless deactivated by the service provider.

In the detailed process descriptions that follow, the initiating user (User "A") has the option of pressing 1, 2 or 3 after receiving recall (stutter) dial tone. In general, the system responds as follows:

- If User "A" presses digit **1**, the remote party currently connected with User "A" is dropped.

- If User “A” presses digit **2**, the remote party currently connected with User “A” is placed on hold, and User “A” is connected to the other remote party.
- If User “A” presses digit **3**, all three parties are immediately bridged into a single voice session (a three-way call).

To Begin a Three-Way Call:

To begin a three-way call, a user involved in a stable two-way call takes the following steps:

- The user (User “A”) presses the **Flash** button or **hookswitch**. The system places the remote party (User “B”) on hold and provides a recall (stutter) dial tone to User “A”.
- After receiving the recall dial tone, User “A” dials the DN of a third party (User “C”). If User “C” answers the call, User “A” and User “C” can talk privately, and User “B” remains on hold.

Note If the user presses the **Flash** button or **hookswitch** before completing dialing, the original two-way connection is reestablished.

Note If User “C” cannot be reached, or does not answer the call, the system provides the applicable busy tone, error tone, or error message to User “A”. However, the system leaves User “B” on hold regardless of the treatment given to User “A” and User “C”.

- To bridge all three parties, User “A” presses the **Flash** button or **hookswitch**. This places User “C” on hold (and User “B” remains on hold also) and provides a recall dial tone to User “A”. If User “A” presses the digit **3**, all three parties are immediately bridged into a single voice session (a three-way call).

Options While on a Three-Way Call with All Three Parties Bridged Together:

While on a three-way call with all three parties bridged together, User “A” can take one of the following actions:

- To drop User “C” and return to the original conversation with User “B”, User “A” presses the **Flash** button or **hookswitch**. This places both of the other parties on hold and provides a recall dial tone to User “A”. If User “A” presses the digit **1**, User “C” is dropped and the original call between User “A” and User “B” is reestablished.
- To drop User “B” and return to the conversation with User “C”, User “A” presses the **Flash** button or **hookswitch**. This places both of the other parties on hold and provides a recall dial tone to User “A”. If User “A” presses the digit **2**, User “C” is placed on hold, and the original call between User “A” and User “B” is reestablished. User “A” can then drop User “B” using **Flash** and digit **1**, and the call between User “A” and User “C” is reestablished.
- To alternate conversations with User “B” and User “C”, User “A” presses the **Flash** button or **hookswitch**. This places both of the other parties on hold and provides a recall dial tone to User “A”. If User “A” presses the digit **2**, User “C” is placed on hold and the original call between User “A” and User “B” is reestablished. From this point User “A” can press the **Flash** button or **hookswitch**, receive recall dial tone, and press **2** to alternate between the parties. This is the same function as for call waiting deluxe (CWD).

Note During a three-way call, the CWD feature does not work for the party that initiated the three-way call (that is, if a fourth party attempts to reach User "A"). User "A" would not be aware of the additional incoming call attempt. However, CWD would work normally for the two called parties (User "B" and User "C").

To Drop User "C" and Return to the Original Call with User "B":

To speak with User "C" and then drop User "C" and return to the original call with User "B", User "A" (while involved in a stable two-way call) takes the following steps:

- The user (User "A") presses the **Flash** button or **hookswitch**. The system places the remote party (User "B") on hold and provides a recall (stutter) dial tone to User "A".
- After receiving the recall dial tone, User "A" dials the DN of a third party (User "C"). If User "C" answers the call, User "A" and User "C" can talk privately, and User "B" remains on hold.

  Note If User "C" cannot be reached, or does not answer the call, the system provides the applicable busy tone, error tone or error message to User "A". However, the system leaves User "B" on hold regardless of the treatment given to User "A" and User "C".

- To drop User "C" and return to the original conversation with User "B", User "A" presses the **Flash** button or **hookswitch**. This places User "C" on hold (and User "B" remains on hold also) and provides a recall dial tone to User "A". If User "A" presses the digit **1**, User "C" is dropped and the original call between User "A" and User "B" is reestablished.

To Put User "C" on Hold and Return to the Original Call with User "B":

To speak with User "C", and then put User "C" on hold and return to the original call with User "B", User "A" (while involved in a stable two-way call) takes the following steps:

- The user (User "A") presses the **Flash** button or **hookswitch**. The system places the remote party (User "B") on hold and provides a recall (stutter) dial tone to User "A".
- After receiving the recall dial tone, User "A" dials the DN of a third party (User "C"). If User "C" answers the call, User "A" and User "C" can talk privately, and User "B" remains on hold.

  Note If User "C" cannot be reached, or does not answer the call, the system provides the applicable busy tone, error tone or error message to User "A". However, the system leaves User "B" on hold regardless of the treatment given to User "A" and User "C".

- To put User "C" on hold and return to the original conversation with User "B", User "A" presses the **Flash** button or **hookswitch**. This places User "C" on hold (and User "B" remains on hold also) and provides a recall dial tone to User "A". If User "A" presses the digit **2**, User "C" is placed on hold and the original call between User "A" and User "B" is reestablished. From this point User "A" can press the **Flash** button or **hookswitch**, receive recall dial tone, and press **2** to alternate between the parties.

To Drop User "B" and Continue the Call with User "C":

To speak with User "C", and then drop User "B" and continue the call with User "C", User "A" (while involved in a stable two-way call to User "B") takes the following steps:

- The user (User “A”) presses the **Flash** button or **hookswitch**. The system places the remote party (User “B”) on hold and provides a recall (stutter) dial tone to User “A”.
- After receiving the recall dial tone, User “A” dials the DN of a third party (User “C”). If User “C” answers the call, User “A” and User “C” can talk privately, and User “B” remains on hold.

Note If User “C” cannot be reached, or does not answer the call, the system provides the applicable busy tone, error tone or error message to User “A”. However, the system leaves User “B” on hold regardless of the treatment given to User “A” and User “C”.

- To put User “C” on hold and return to the original conversation with User “B”, User “A” presses the **Flash** button or **hookswitch**. This places User “C” on hold (and User “B” remains on hold also) and provides a recall dial tone to User “A”. If User “A” presses the digit **2**, User “C” is placed on hold and the original call between User “A” and User “B” is reestablished.
- To drop User “B” and return to the conversation with User “C”, User “A” presses the **Flash** button or **hookswitch**. This places User “B” on hold (and User “C” remains on hold also) and provides a recall dial tone to User “A”. If User “A” presses the digit **1**, User “B” is dropped and the call between User “A” and User “C” is reestablished.

TWCD Feature Behavior When a Party Disconnects:

When a three-way call has been established with all three parties bridged together, the following actions take place when one of the parties disconnects (hangs up):

- If User “A” (the TWCD-initiating party) disconnects, all connections are dropped, unless User “A” is also subscribed to CT (see the “TWCD Feature Interactions” section on page 3-126).
- If User “B” disconnects, a two-way call continues between User “A” and User “C”.
- If User “C” disconnects, a two-way call continues between User “A” and User “B”.

Note When User “B” or User “C” disconnects, and User “A” is in a two-way call with the remaining party, User “A” can initiate a new three-way call using the procedures described above.

TWCD Timers

There are two timers that apply to the TWCD feature:

- Feature reconnect timer (FEATURE-RECONNECT-TMR), measured in seconds—During the course of using the TWCD feature, if the subscriber is connected to a reorder tone or announcement, the subscriber is automatically reconnected to the previous call leg after the specified FEATURE-RECONNECT-TMR timeout period. The default value is 10.
- Reconnect timer (RECONNECT-TMR), measured in seconds—When a subscriber hangs up with another call on hold, the subscriber is rung back. The ringing is applied for the duration of this RECONNECT-TMR. If the subscriber does not answer the call within this time period, the call is torn down. The default value can be provisioned in the CA-CONFIG table. If the timer is not provisioned in the CA-CONFIG table, the preset value 36 is used as default.

Invalid User Actions

The valid user actions are described in the sections above. The following user actions are invalid, and the system provides an appropriate error announcement:

- The user presses the Flash button or hookswitch, receives recall dial tone, and then enters a DN that is invalid.
- The user presses the Flash button or hookswitch, receives recall dial tone, and then enters a digit other than 1, 2, or 3.

TWCD Feature Interactions

TWCD and TWC interaction

When TWCD and TWC are assigned to the same line, TWCD has higher precedence than TWC.

TWCD and CT Interaction

If TWCD and CT are assigned to the same line, CT has higher precedence than TWCD.

When the TWCD-initiating party hangs up during a TWCD, and the TWCD-initiating party is not subscribed to call transfer (CT), all parties are disconnected.

However, if the TWCD-initiating party is also subscribed to CT (as provisioned in the subscriber-feature-profile table), the two remaining parties stay connected. The following scenarios occur, depending upon the actions of the parties in the call. In these scenarios, User A is subscribed to both CT and TWCD and is the TWC-initiating party, B is the party in the initial established call with A, and C is the third party:

- User A is in a stable call with B, places B on hold and dials C.
- If A hangs up after successfully dialing C (C is ringing), a two-way call is established between B and C, regardless of whether C answers the call. User A is billed for a call transfer, but is not billed for the time that the other two parties are on the call.
- If A waits until C answers the call, and then A hangs up, a two-way call is established between B and C. User A is billed for a call transfer and is also billed for the entire duration starting from the time A initiated the TWC until B and C hang up.

TWCD and CWD Interaction

The invocation of these two features is mutual exclusive. When one feature is invoked, the other feature is not allowed.

Note During a three-way call, the CWD feature does not work for the party that initiated the three-way call. However, the CWD feature would work normally for the other two (non-initiating) parties.

TWCD and OCB Interaction

When TWCD and OCB are assigned to the same line, and if OCB is activated, when the user presses the Flash button or hookswitch to make a second call, the second call is subject to OCB screening.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the TWCD provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Usage-Sensitive Three-Way Calling (USTWC)

The Cisco BTS 10200 Softswitch supports usage-sensitive three-way calling (USTWC) feature as specified in LSSGR module FSD 01-02-1304 (TR-TSY-000578), *Usage-Sensitive Three-Way Calling*.

Limitations

If your network uses an ISUP variant other than ANSI ISUP, the system supports TWCD, but not TWC or USTWC.

Feature Description

USTWC allows a user to add a third party to an existing two party conversation. It provides all the functionality of TWC (see the "Three-Way Calling (TWC)" section on page 3-121) without requiring the user to subscribe to the service. The service provider may charge differently for the use of this service. The usage-sensitive features can be enabled/inhibited per user by turning on/off the usage-sensitive option for the user.

The user activates and uses this service in the same manner as TWC.

Note The USTWC feature can be made available to all subscribers lines connected to a BTS 10200 using the default office service ID, or to all subscribers in a specific POP using the office service ID. See the "Office Service ID and Default Office Service ID" section on page 3-134 for a general description of this provisionable service.

Feature Provisioning Commands

Provisioning commands are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision this feature, see the USTWC provisioning procedure in the Cisco BTS 10200 Softswitch documentation set.

Visual Message Waiting Indicator (VMWI)

See the "Message Waiting Indicator (MWI)—Audible and Visual" section on page 3-89.

Voice Mail (VM) and Voice Mail Always (VMA)

The BTS 10200 supports Voice Mail (VM) and Voice Mail Always (VMA) features for individual, Centrex, and MLHG subscribers. These features allow subscribers to:

- Forward calls to voice mail when subscribers are busy, or when subscribers do not answer the phone. This is referred to as VM.
- Forward all calls to voice mail regardless of the subscriber's phone status and without attempting to ring the subscriber's phone. This is referred to as VMA.
- Dial designated VSC codes to activate/deactivate the feature, and dial a dedicated DN (or use a designated VSC) to access the voice mail server to retrieve their messages. If activated, the VSC serves as a shortcut to voice mail.

VM and VMA have interactions with all of the other call-forwarding features (CFU, CFB, CFNA, and CFC). The following interactions apply for these features when activated:

- If activated, CFU takes precedence over both VM and VMA.
- If activated, CFB, CFNA, and CFC all take precedence over VM.
- VMA takes precedence over CFB, CFNA, and CFC.

Some caveats apply to the above list of interactions. See the "Feature Interactions" section on page 3-132.

Note The system does not support VM or VMA managed by the GUI Feature Server for IP phones in this release.

VM Activation, Deactivation, and Invocation

This section describes VM activation, deactivation, and invocation.

VM Activation

The subscriber activates VM on the phone by:

1. Picking up the phone, and hearing a dial tone.
2. Dialing the VM Activation access code.

The subscriber hears an appropriate announcement depending on whether the activation was successful or not.

The activation attempt fails for the following scenarios. In these cases, the subscriber hears an appropriate error announcement if:

- VM is not assigned to the subscriber.
- VM is already active.

A success activation attempt results in a confirmation announcement.

Note When assigned, VM is considered activated unless explicitly deactivated by either the subscriber or the operator.

VM Deactivation

The subscriber deactivates VM on the phone by:

1. Picking up the phone, and hearing a dial tone.
2. Dialing the VM Deactivation access code.

The subscriber hears an appropriate announcement based on whether the deactivation was successful or not. The deactivation attempt fails for the following scenarios; in these cases, the subscriber hears an appropriate error announcement:

- VM is not assigned to the subscriber.
- VM is already deactivated.

A success deactivation attempt results in a confirmation announcement.

VM Invocation

If the subscriber is either busy or does not answer the phone, incoming calls to a subscriber who has VM activated are forwarded to a voice mail server where the caller is guided to leave a message. The subscriber can later retrieve the message.

VMA Activation, Deactivation, and Invocation

This section describes VMA activation, deactivation, and invocation.

VMA Activation

The subscriber activates VMA on the phone by:

1. Picking up the phone, and hearing a dial tone.
2. Dialing the VMA Activation access code.

The subscriber hears an appropriate announcement depending on whether the activation was successful or not.

The activation attempt fails for the following scenarios. In these cases, the subscriber hears an appropriate error announcement if:

- VMA is not assigned to the subscriber.
- VMA is already active.

A success activation attempt results in a confirmation announcement.

Note When assigned, VMA is considered deactivated unless explicitly activated by either the subscriber or the operator.

VMA Deactivation

The subscriber deactivates VMA on the phone by:

1. Picking up the phone, and hearing a dial tone.
2. Dialing the VMA Deactivation access code.

The subscriber hears an appropriate announcement based on whether the deactivation was successful or not. The deactivation attempt fails for the following scenarios; in these cases, the subscriber hears an appropriate error announcement:

- VMA is not assigned to the subscriber.
- VMA is already deactivated.

A success deactivation attempt results in a confirmation announcement.

VMA Invocation

Incoming calls to a subscriber who has VMA activated are forwarded to a voice mail server where the caller is guided to leave a message. The subscriber can later retrieve the message.

VM Access

The VM Access subfeatures allow the subscriber to retrieve messages by dialing the VM Access code. The procedure is as follows:

1. If the subscriber has a new message waiting, the system plays a stutter dial tone when the phone goes off-hook. Alternatively, if the subscriber has the visual message waiting indicator (VMWI) function assigned and active, the indicator light goes on.
2. The subscriber picks up the phone and dials the VM Access code. If successful, subscriber is guided through a menu to manage the messages.

   Access can fail for the following scenarios. In these cases, the subscriber hears an appropriate error announcement.

   - The subscriber is not assigned the VM Access subfeature.
   - The service provider has not assigned an Access Code for the VM Access subfeature.

Tip For information on message waiting indicators, typically used in conjunction with VM and VMA, see the "Message Waiting Indicator (MWI)—Audible and Visual" section on page 3-89.

Provisionable Parameters for VM and VMA

This section provides information on several tables and parameters that affect the behavior of the VM and VMA features.

Feature Table

VM and VMA are implemented by provisioning the following features in the feature table:

- VM
- VM_ACT
- VM_DEACT
- VMA
- VMA_ACT
- VMA_DEACT
- VM_ACCESS

The feature table contains two parameters that affect VM/VMA behavior:

- Multiple call forwarding (MCF) parameter (applicable to both VM and VMA)—There can be multiple voice mail sessions active on a subscriber at one time based on the MCF flag. If the MCF flag is set to Y (default value), multiple concurrent sessions to voice mail are allowed. If the MCF flag is set to N, the system rejects subsequent sessions to voice mail, and the caller hears a busy tone or a busy announcement. The Voice Mail Application Server can support multiple incoming calls for the same subscriber.
- Timeout (TO) parameter (applicable to VM only)—TO denotes the number of seconds the system waits for the subscriber to answer an incoming call before forwarding the call to voice mail. The default value for TO is 30 seconds (approximately 6 rings). Although the system does not block provisioning a higher TO value, the recommended range for TO is from 6 to 180 seconds.

Note There is also a TO parameter in the subscriber-feature-data table. If both the subscriber-feature-data and feature tables have the TO value provisioned, the system uses the value provisioned in the subscriber-feature-data table.

VSC Provisioning

The Vertical Service Code (VSC) is provisionable and can be any unique valid string of ASCII characters; for example, *222.

VM Forwarding Directory Number

There are two directory numbers (DNs) provisioned in the Application Server (app-server) table:

- APP-SERVER-DN—This is the voice-mail directory number (DN), and is used to forward an incoming call to the voice mail server.
- APP-SERVER-ACCESS-DN—This is the DN used when the subscriber accesses the VM/VMA management features to change the VM settings. If this token is not provisioned, it defaults to the value provisioned for APP-SERVER-DN.

Note Subscribers cannot set or change the DNs for the application server or application server access.

Additional features of the app-server table are as follows:

- The APP-SERVER-TYPE token must be set to VM to identify this server as a voice-mail server.
- The system can be provisioned to access multiple VM servers.
- The ID of the app-server table is indexed (as the VOICE-MAIL-ID token) in the Subscriber (subscriber), Subscriber Profile (subscriber-profile), and POP (pop) tables. The system applies the following rules when selecting the specific app-server table applicable to a particular subscriber:
  - If the subscriber and subscriber-profile tables are indexed to different app-server IDs (VOICE-MAIL-ID token), the app-server in the subscriber table is used.
  - If the subscriber-profile and pop tables are indexed to different app-server IDs, the entry pointed to by the subscriber-profile table is used.
  - If the pop and ca-config tables are indexed to different app-server IDs, the entry pointed to by the pop table is used.

– If the app-server ID (VOICE-MAIL-ID token) is not provisioned at any level (subscriber, subscriber-profile, or pop), the system uses the switch-level default app-server ID (TYPE=DEFAULT-VOICE-MAIL-ID) provisioned in the Call Agent Configuration (ca-config) table.

Feature Provisioning Procedure

Provisioning procedures are available in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip To provision the VM and VMA features, see the VM provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Feature Interactions

The following interactions between features is implemented as a part of this feature development.

- CFU, CFB and CFNA:

  Table 3-26 summarizes these interactions.

Table 3-26 VM and VMA Interactions with Call-Forwarding

Voice Mail Features Active	Forwarding Features Active	Interaction
VM	CFU	Call is forwarded by CFU.
VM	CFB	Calls on which the subscriber is busy are forwarded by CFB. Calls on no answer from the subscriber are forwarded by VM.
VM	CFNA	Calls when subscriber is away from the phone are forwarded by CFNA. This is true even if the CFNA timeout is greater than the VM timeout. Calls when the subscriber is busy are forwarded by VM.
VM	CFU and (CFB or/and CFNA)	Call is forwarded by CFU.
VMA	CFU	Call is forwarded by CFU.
VMA	CFB or/and CFNA	Call is forwarded by VMA
VMA	CFU and (CFB or/and CFNA)	Call is forwarded by CFU.
VM and VMA	CFU	Call is forwarded by CFU.
VM and VMA	CFB or/and CFNA	Call is forwarded by VMA.

- Selective Call Acceptance/Rejection Features (SCA, SCR)

  If the call is accepted by SCA or not rejected by SCR, then the call is forwarded by VM if the subscriber is busy or does not answer within the VM timeout. Also, if accepted by SCA/SCR, the call is forwarded to voice mail if the subscriber has VMA active. If the call is not accepted by SCA or rejected by SCR, the call does not go to voice mail.

- Selective Call Forwarding

If an incoming call is not selectively forwarded (i.e., the call terminates on the subscriber's phone), the call is forwarded by VM if the subscriber is busy or does not answer within the VM timeout. Also, if an incoming call is not selectively forwarded (i.e., the call terminates on the subscriber's phone), the call is forwarded to voice mail if the subscriber has VMA active. If the call is selectively forwarded, it does not go to voice mail.

- Do Not Disturb

  If a subscriber has DND and VM assigned and active, the call is redirected by VM.

  If a subscriber has DND and VMA assigned and active, the call is redirected by VMA.

- Anonymous Call Rejection

  If the call is accepted ACR, then it is forwarded by VM if the subscriber is busy or does not answer within the VM timeout. Also, if the call is accepted by ACR, then it is forwarded by VMA if the subscriber has VMA active. If the call is rejected, it does not go to voice mail.

- Abbreviated Dialing/Speed Call

  The subscriber can provision the speed call or abbreviated dial to the VM/VMA activation, deactivation or access codes. The subscriber can then invoke any of these features by dialing the speed code or the abbreviated dial numbers.

- Voice Mail and CW/CIDCW/CWD

  The subscriber can send calls to voice mail if already on a call. If the subscriber has CW/CIDCW/CWD and does not answer an incoming call, the call is redirected by VM/VMA if active.

  It is important to be aware of several provisionable parameters that can further affect the processing of this call.

  – The CW timeout is based on a switch-wide parameter, NO-ANSWER-TMR in the ca-config table (default 185 seconds). There is also a parameter, START-NO-ANSWER-TMR in the ca-config table, to specify whether NO-ANSWER-TMR is to be started or not; default is N.

    The VM timeout is provisioned via the TYPE1=TO parameter in the Feature table (default 4 seconds).

  – If Subscriber A has the default timer settings (that is, VM TO=4 seconds and NO-ANSWER-TIMER=185 seconds), and has the START-NO-ANSWER-TMR parameter set to Y (not the default), the call is processed as follows:

    [1] A calls B, B answers.

    [2] C calls A, A hears the CW tone, C hears ring tone.

    [3] If A does not attempt to answer the waiting call (C), and VM times out (4 seconds), C is forwarded according to normal VM forwarding procedures.

    However, if the VM timeout (TO) is set to a value *greater than* NO-ANSWER-TMR, when NO-ANSWER-TMR expires, C is disconnected and hears a busy tone, and VM is cancelled.

- There is an interaction when a Centrex subscriber has all three of the following features assigned and active:

  1. Call hold—CHD.
  2. Call waiting—CW or CIDCW or both.
  3. Call forwarding on no answer—CFNA, VM (or VMA), or any combination of these.

  For information on this interaction, see the "CHD with CW/CIDCW and CFNA/VM/VMA" section on page 3-70.

- Hotline/Warmline/HOTV

  The subscriber cannot provision hotline or warmline/HOTV features to the VM/VMA activation, deactivation or access codes.

- COS/OCB and Voice Mail

  The system does not apply COS or OCB screening to calls which are redirected to voice mail or when the subscriber accesses the voice mail.

Warmline Service

Warmline service is a combination of hotline service (see the "Hotline Service" section on page 3-81) and regular phone service on the same line. The service is activated by the service provider at the request of the subscriber. The service provider provisions a timeout parameter in the FEATURE table (default is 4 seconds), and the warmline service uses that timeout value as follows:

- Use of warmline for regular phone service—The user takes the handset off hook, receives dial tone, and starts dialing a regular call before the timeout expires.
- Use of warmline as a hotline—The user takes the handset off hook, receives dial tone, but does not dial any digits. After the timeout expires, the system automatically calls the predetermined DN.

Note This timeout is a switch-level timeout common to all subscribers, and normally not changed on a per-subscriber basis.

Note This variable timeout feature operates with MGWs that are compliant with MGCP1.0 (per IETF document *RFC 2705*) or higher. For MGWs compliant with MGCP0.1 only, the timeout is not variable.

Certain limitations apply to the use of the warmline feature:

- An exclusive telephone DN is required for the warmline feature.
- None of the VSC star (*) features are available on this line

Only the service provider can deactivate warmline service

Tip To provision this feature, see the Warmline provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Office Service ID and Default Office Service ID

One service ID (the office service ID) is reserved for provisioning of POP-based features. These office-based features can include certain network features and certain usage-sensitive features, as described below. The service provider provisions the individual features, enters a unique ID in the service table, and provisions this service ID in the POP table. All of the subscribers within the POP are provided with this service (and this set of features).

One service ID (the default office service ID) is reserved for provisioning of switch-based features. The service provider provisions the individual features, enters a unique ID in the service table, and provisions this service ID in the CA-Config table. All of the subscribers on the switch are provided with this service (and this set of features).

Note If the office-service-id is provisioned in the POP table, the system uses this value. However, if the office-service-id is *not* provisioned in the POP table, the system uses the default-office-service-id provisioned in the CA-Config table.

Caution The system does not validate or restrict the provisioning of features on the office service ID. However, entries other than the ones listed below will have undefined results. Do not enter features other than the ones listed below.

The following features can be provisioned with the office-service-id (POP table) and the default-office-service-id (CA-Config table):

- USTWC (For three-way-calling, note that USTWC is the feature that can be included in the office service ID, and TWC is the feature that can be assigned to individual subscribers.)
- COT
- AR_ACT (or AR, if umbrella feature was created)
- AR_DEACT (not needed if umbrella feature AR was created)
- AC_ACT (or AC, if umbrella feature was created)
- AC_DEACT (not needed if umbrella feature AC was created)
- 8XX
- LNP
- 911
- BLV
- REFER—Valid for SIP subscribers only
- REPLACES—Valid for SIP subscribers only

Tip To provision the office service ID, see the Office Service ID provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Notes on Bundling Features in Services

The service provider can bundle features and services as follows:

- Associated features can be bundled with their primary feature (for example, the call waiting deluxe (CWD) associated features CWD activation, CWD deactivation, and CWD interrogation, can all be bundled with the CWD feature)
- Groups of features can be bundled into service packages (services)

Provisioning procedures for features and services are presented in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

CHAPTER 4

Class of Service Restrictions and Outgoing Call Barring Features

Revised: March 24, 2011, OL-12606-21

The Cisco BTS 10200 Softswitch supports class of service restrictions and call barring options on outgoing calls. There are two suites of call restrictions—Class of Service (COS) restrictions and Outgoing Call Barring (OCB). The COS and OCB features are assigned by the service provider. The COS feature cannot be controlled or deactivated by individual subscribers. The OCB feature can be activated, controlled, and deactivated by individual subscribers. These features are discussed in the following sections:

- "Class of Service Restrictions" section on page 4-1
- "Outgoing Call Barring (OCB)" section on page 4-14

Note For information on network features, see Chapter 1, "Network Features."

For information on subscriber features, see Chapter 3, "Subscriber Features."

Caution Some features involve the use of other network elements (NEs) deployed in the service provider network, for example, gateways, media servers, announcement servers, eMTAs, and SIP phones. See the "Component Interoperability" section of the *Release Notes* for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the BTS 10200 Release 5.0 software. Earlier or later releases of platform software might be interoperable and it might be possible to use other functions on these platforms. The list in the *Release Notes* certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the BTS 10200.

Class of Service Restrictions

The BTS 10200 supports class of service (COS) restrictions on certain call types. The COS feature is assigned by the service provider and cannot be controlled or deactivated by individual subscribers.

This section covers the following topics:

- How to Use This Section of the Document

- COS Functional Description
- Exemptions from COS and OCB Restrictions
- National Call Restrictions (Toll Restrictions)
- Overview—Black and White List Features
- Casual Call (101XXXX) White and Black Lists (Number Blocking)
- National White and Black Lists (Number Blocking)
- International White and Black Lists (Number Blocking)
- Originating Line Information White and Black Lists
- Nature of Dial White and Black Lists
- Blocking Flags
- Account Codes and Authorization Codes
- ANI Screening on Incoming Calls
- Temporary Disconnect Treatment
- COS Restriction Priorities
- High-Level Flowchart of COS Screening Process

How to Use This Section of the Document

This section describes the COS feature and the impact of certain provisionable parameters. For the basic sequence of commands used to provision this feature, see the COS provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

COS Functional Description

COS restrictions prevent certain types of calls from being completed from a particular line or station. The service provider can:

- Provision COS restrictions for individual subscribers, groups of subscribers, trunk groups (TGs), automatic number identification (ANI), and authorization codes.
- Prohibit calls based on dialing plans and call types. (Call types for COS screening are contained in the Nature of Dial (NOD) table.)

When a call is blocked, the calling party receives a blocking treatment such as reorder tone or announcement.

Exemptions from COS and OCB Restrictions

Certain types of calls are exempt from both COS and OCB restrictions:

- Emergency calls (calls with call-type=EMG)—These calls are never subject to COS and OCB screening. The system always exempts emergency calls from COS and OCB screening without considering any provisioned parameters. Note that it is possible to provision AMBULANCE, FIRE, and POLICE as subtypes of EMG in the Destination table. If provisioned as subtypes of EMG, these types are given the same treatment as EMG.

- Call types on either of the NOD exception lists—The service provider can provision exception lists to override COS and OCB screening on certain types of calls. The types of calls on these lists can include, for example, repair calls, toll-free calls, and so forth. The applicable types of calls are listed in the NOD table. These exceptions are applicable at the switch level (all office codes) and cannot be specified for individual subscribers. There are two NOD exception lists:
  - Trigger NOD Escape List table—If the service provider provisions a NOD type/trigger ID pair in the Trigger NOD Escape List (trigger-nod-escape-list) table, that NOD type will not trigger COS or OCB screening.
  - NOD Restrict List—If the service provider provisions a NOD type in the NOD Restrict List (nod-restrict-list) table, that NOD type can trigger COS or OCB screening, but will be exempted at the first screening step.

Tip Cisco recommends that you use trigger-nod-escape-list to provide this function, because it uses system resources more economically. It is not necessary to provision both lists for this function.

See the complete list of NOD values in the Nature of Dial table in the *Cisco BTS 10200 Softswitch CLI Database*.

National Call Restrictions (Toll Restrictions)

The national call restrictions are used to allow or restrict calls to destinations based on a predefined grouping of local lines, LATA, state, country, or group of countries. Customers can subscribe to one of the following:

- All North American Numbering Plan (NANP) calls—All calls within NANP are allowed (can be applied only to calls originated in NANP).
- National only—Only calls terminating within the country are allowed.
- Intrastate only—Only calls within the state are allowed.
- IntraLATA only—Only calls within the LATA are allowed, including intraLATA toll calls (can be applied only to calls originated in NANP).
- Local only—Only local calls are allowed.

For NANP operator calls (0+NPA-NXX-XXXX), NANP call restriction screening is not performed, even if the NANP call restriction is provisioned in the cos-restrict table for the calling party.

Overview—Black and White List Features

The service provider can provision a list of directory numbers (DNs) to appear on a black list or a white list as follows:

- Black-listed calls do not undergo further screening, and all calls on this list are rejected. This is called number blocking.
- White-listed calls are subject to additional normal OCB restrictions based on call type (if the OCB feature is assigned to the subscriber and activated).

The service provider can also create white and black lists based on originating line information (OLI) and nature of dial (NOD).

Note OCB is a subscriber feature that the service provider can assign to any subscriber line. After OCB is assigned, it is controlled by the individual subscriber. (Typically, OCB is used by service providers outside the North American market.)

For the black/white-list functionality of the OCB feature, the service provider should provision the desired black/white-list COS restrictions for each OCB subscriber, and assign a COS-RESTRICT-ID for the subscriber. This ensures that the black and white list restrictions are in effect, even if the user deactivates OCB. For a complete description of the OCB feature, see the "Outgoing Call Barring (OCB)" section on page 4-14.

The service provider can provision an exception list to override COS and OCB screening on certain types of calls. See the "Exemptions from COS and OCB Restrictions" section on page 4-2.

For details on each type of black/white list, see the following sections:

- Casual Call (101XXXX) White and Black Lists (Number Blocking)
- National White and Black Lists (Number Blocking)
- International White and Black Lists (Number Blocking)
- Originating Line Information White and Black Lists
- Nature of Dial White and Black Lists
- Blocking Flags

Casual Call (101XXXX) White and Black Lists (Number Blocking)

The casual call white and black lists are used to allow or restrict calls dialed with a casual code prefix (101XXXX). The applicable COS can be set up to perform either white list screening or black list screening, but not both. The following restrictions can be provisioned:

- No casual calls allowed—User cannot make 101XXXX calls.
- All casual calls allowed—User can make 101XXXX calls.
- 101XXXX white list—Only a predefined set of XXXX codes can be dialed.
- 101XXXX black list—All XXXX codes can be dialed except for a predefined set.

For NANP operator calls (0+NPA-NXX-XXXX) and international operator calls (01+CC+NN), casual-call screening is not performed, even if the casual-call restriction is provisioned in the cos-restrict table for the calling party.

National White and Black Lists (Number Blocking)

The national white and black lists are used to allow or block national calls based on a predefined list of DNs. The applicable COS can be set up to perform either white list screening or black list screening, but not both. The following restrictions can be applied:

- No restrictions.
- National white list—Only calls on a predefined prefix list can be called. The list could consist of full or partial DNs (for example, NDC or NDC-EC codes, or NPA or NPA-NXX codes for North America).

- National black list—All calls on a predefined prefix list are blocked. The list could consist of full or partial DNs (for example, NDC or NDC-EC codes, or NPA or NPA-NXX codes for North America).

For NANP operator calls (0+NPA-NXX-XXXX), NANP call restriction screening is not performed, even if the NANP call restriction is provisioned in the cos-restrict table for the calling party.

The national white black list table checks telephone numbers only for the following call types: local, intralatatoll, interlatatoll, national (ITU only), toll, intl-wz1, international, casual, 900, premium, 976, da, da-toll, 0-plus, 0-minus, 01-plus, tw, info and non-emergency. The system does not check this list if the NOD is not one of these call types. For example, if an 800 number is added to this table, the number is not checked, since an 800 number is call type toll-free, and toll-free is not a supported call type.

International calls within NANP are screened against the national white and black lists, and not against the international white and black lists.

International White and Black Lists (Number Blocking)

The international white and black lists are used to allow or block calls made outside the country. The applicable COS can be set up to perform either white list screening or black list screening, but not both. The following restrictions can be applied:

- No international calls allowed—Does not allow any international calls.
- International white list—Allows only those calls that have a country code (CC) noted in the white list.
- International black list—Does not allow any calls that have a CC noted in the black list.
- All international calls allowed—No restrictions are applied on international calls.

For international operator calls (01+CC+NN), international call restriction screening is not performed, even if the international call restriction is provisioned in the cos-restrict table for the calling party.

International calls within NANP will be screened against the national white and black lists, and not against the international white and black lists.

Originating Line Information White and Black Lists

The originating line information (OLI) white and black lists (also referred to as II white and black lists) are used to allow or block calls made from certain types of lines, such as hotels, prisons, and so forth. This is a Tandem call screening function. The applicable COS can be set up to perform either white list screening or black list screening, but not both. The following restrictions can be applied:

- No OLI screening performed.
- Use the II white/black screening list as a white list—Allows the specified OLI types to place calls.
- Use the II white/black screening list as a black list—Blocks calls from the specified OLI types.

Note II digits 24 and 25 are exempt from COS screening (these are translated toll-free 8XX calls from POTS lines).

Nature of Dial White and Black Lists

The nature of dial (NOD) white and black lists (NOD-WB-LIST) are used to allow or block certain categories of calls, such as casual dialing (dialing around), time/weather, international operator assistance, premium calls, toll calls, toll-free calls, and so forth. The following restrictions can be applied:

- No NOD screening performed.
- Use the NOD white/black screening list as white list—Allow the specified NOD types to be called.
- Use the NOD white/black screening list as black list—Block calls to the specified NOD types.

To block international calls that originate within the 48 contiguous U.S. states and terminate in World Zone 1 (outside of the contiguous 48 states but within NANP), set the NOD token to INTL-WZ1 in the NOD White Black List table.

Certain types of calls that are exempt from both COS and OCB restrictions. See this information in the "COS Functional Description" section on page 4-2.

Refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for a complete list of NOD types.

Blocking Flags

The service provider can provision the blocking flags listed below. These have the same effect as provisioning the NOD black list for the same feature.

Tip All call types that can be blocked using blocking flags can *also* be blocked by placing that call type on the NOD black list. Cisco recommends using the NOD black list.

- Block 900 (premium) calls—Blocks all calls of the form 1-900-XXX-XXXX.
- Block 976 (local information) calls—Blocks all calls of the form 976-XXXX or NPA-976-XXXX.
- Block info calls—Blocks all calls to information services.
- Block time/weather calls—Blocks all calls to time and weather services.
- Block directory assistance (DA) calls—Blocks all directory assistance calls of the form 411, 1+411 or NPA-555-XXXX.
- Block NANP operator assistance calls—Blocks all calls to an operator within NANP, specifically, 0 calls and 0+ calls (0+NPA-NXX-XXXX).
- Block international calls—The behavior of this flag depends upon the location of the originating station:
  - For call that originate from locations outside NANP, this flag blocks all calls terminating outside the country.
  - For calls that originate from locations inside NANP, this flag blocks all calls terminating outside NANP.

Note For calls that originate from locations inside NANP, to block calls terminating outside the country but inside NANP (for example, calls from the United States to Canada), use the INTL-WZ1 token in the NOD White Black List.

- Block international operator assistance calls—Blocks all calls to an operator outside the country, including 01+ calls (01+CC+NN).

Account Codes and Authorization Codes

The BTS 10200 supports account code and authorization code features as described in this section. These features are part of the COS features, and include the collection and screening of digits on calls. The individual or business can use this feature to help restrict or block certain types of outgoing calls.

Tone-Based and IVR-Based Options

The service provider can provision the system to use either a tone-based procedure or an IVR-based procedure for collecting and screening the digits.

Note Cisco recommends that you use IVR-based COS only in cases where the originating MGW or TGW is unable to play tones to the caller. The IVR-based COS feature for ISDN trunk is for the North American market only. It is not supported for SS7, H.323, or SIP endpoints.

- The tone-based procedure requires that the originating MGW be capable of playing tones to the caller. When an account or authorization code is required during COS screening, the BTS 10200 instructs the MGW to play the appropriate tones and collect digits. After the digits are collected, the call proceeds or is blocked based on COS restrictions.
- The IVR-based procedure is used when the originating MGW is not capable of playing tones to the caller. This is typically true of TGWs and devices such as PBXs connected over ISDN PRI trunks at the customer premises. When an account or authorization code is required during COS screening, an IVR server plays the appropriate prompts and collects digits entered by the handset user. After the digits are collected, the call proceeds or is blocked based on COS restrictions.

Tone-Based Operation

This section describes the tone-based operation of account codes and authorization codes. It also describes provisionable prompt-delay timers that can be used for certain scenarios involving PBX systems.

Account Codes (Nonverified) Tone-Based Operation

Account codes provide collection of 2 to 12 digits to allow call charging to user projects, departments or special accounts. The user activates account codes by dialing a number (usually a long-distance call) that requires an account code for call completion. A prompt tone is issued after the digits are dialed. The user then enters an account code of a specified length. These account codes are not verified. (See the next section for verified account codes.) The account code is provided in the call detail records (CDRs) associated with the call. Account codes are not collected for any of the following call types:

- National operator calls
- International operator calls
- Local calls

For Release 5.0, Maintenance Release 1, and later, the following additional capabilities are added. They are provisionable in the feature-config table:

- The system can allow or inhibit the collection of account codes for calls with nature of dial (NOD) types LOCAL, NON-EMG, and TOLL-FREE.
- The system can be provisioned to apply an account-code prompt delay for calls originating from NCS endpoints.

Authorization Codes (Verified Account Codes)—Tone-Based Operation

Authorization codes, also referred to as verified account codes, can be used by an intended user or group to override certain COS calling restrictions. For example, long-distance calls could be restricted on certain phones, such as phones in a lobby or conference room, unless the user knows a valid authorization code. When an authorization code is required, the user is prompted via a tone. The user can override the restriction by dialing an authorization code that has enough privileges to make long-distance calls. Authorization codes can be from 3 to 23 digits in length.

The user takes the following action when an authorization code is required:

- The user goes off hook and receives a dial tone.
- The user dials a DN. The system determines that an authorization code is required and returns a confirmation tone (2 beeps) to the user.
- The user enters the digits for the authorization code.
  - If the user enters the correct authorization code, the call is screened based on COS assigned to that authorization code. If this authorization code has appropriate privileges, the call is allowed.
  - If the user enters a code that is incorrect, does not have appropriate privileges for the call being attempted, or if the associated account is invalid, the call is diverted to a preselected announcement.

Authorization codes can be used to override call category restrictions, but cannot be used to override black/white lists. For example, an authorization code can be used to override “no international calls allowed”, but cannot be used to override any type of black/white list.

Use of Prompt-Delay Timers for PBX System Connected via IAD

When an account code or authorization code is required, a caller connected to an IAD or MGW is provided with a prompting tone. However, if a caller is connected to a PBX that is connected to an IAD (via CAS protocol), the PBX might not be capable of cutting through the prompting audio quickly enough for the caller to actually receive the prompt. To help resolve this problem, the BTS 10200 has provisionable tokens that can be used to introduce delay before playing the account-code or authorization-code prompt. When this prompt delay is provisioned appropriately, PBX users are able to hear the confirmation tone when they make calls requiring an access code. The option to delay the MGCP RQNT message applies only to CAS trunk groups without main-subscriber, or CAS trunk groups with main-subscriber whose category is PBX. The delay is provisionable via CLI using the following tokens in the CA-CONFIG table:

- ACCT-CODE-PROMPT-DELAY, for introducing delay prior to playing the account code prompt.
- AUTH-CODE-PROMPT-DELAY, for introducing delay prior to playing the authorization code prompt.

Note The prompt-delay feature is not supported for SS7, H.323, ISDN, or SIP endpoints, or for analog subscriber lines.

For detailed descriptions of these tokens, see the *Cisco BTS 10200 Softswitch Command Line Reference Guide*. For a list of commands used to provision these features, see the *Cisco BTS 10200 Softswitch Provisioning Guide*.

IVR-Based Operation

The system supports IVR-based operation of account codes and authorization codes for ISDN trunks. The feature interfaces with, and is dependent on, the services of a network IVR server. When an account or authorization code is required during COS screening, an IVR voice path is established between the IVR server and the ISDN trunk on the TGW/MGW/IAD at the customer site.

Prerequisites for IVR-Based Operation

For IVR-based capabilities, the BTS 10200 interfaces with, and is dependent on, the services of an IVR server. The feature also requires all the network setup for a basic feature call. This feature further requires the PacketCable Basic Audio Package (BAU) interface for managing and controlling IVR endpoints. See PacketCable document PKT-SP-ASP-102-010620.

Restrictions and Limitations for IVR-Based Operation

The following restrictions and limitations apply to the implementation of the IVR-based COS account and authorization codes:

- The IVR-based account and authorization code capability is supported only for ISDN PRI trunks and only in the North American market.
- The system does not support the IVR-based account and authorization code capability for SS7, H.323, and SIP endpoints.
- The system does not support local IVR capability. (Local-IVR involves using IVR resources of the ingress gateway.)
- In the BTS 10200, authorization and account codes reported using IVR are not appended to the *DialedDigit* parameter issued to billing record because the IVR digits are not processed in the Call Agent.

Feature Provisioning

The following tokens in the Class of Service Restrict (cos-restrict) table affect the behavior of this feature:

- To control the type of prompt played to the user, set the PROMPT-METHOD token to TONE (default) or IVR.
- To specify whether to permit calls when an IVR server fails, set the ALLOW-CALLS-ON-IVR-FAILURE token to Y (default) or N.
- Account code parameters—ACCT-CODE-ALLOW and ACCT-CODE-LENGTH.
- Authorization code parameters—AUTH-CODE-ALLOW, AUTH-CODE-LENGTH, and AUTH-CODE-GRP-ID. The following tables are also necessary for authorization code—Authorization Code (auth-code) and Authorization Code Group (auth-code-grp).

The following tokens in the Feature Configuration (feature-config) table can be adjusted if necessary for treatment of account codes:

- ALLOW-NCS-ACCT-CODE-PROMPT, LOCAL-NOD-ACCT-CODE-COLLECT, TOLLFREE-NOD-ACCT-CODE-COLLECT, NON-EMG-NOD-ACCT-CODE-COLLECT.

The following tokens in the Call Agent Configuration (ca-config) table can be adjusted if necessary for treatment of account codes and authorization codes:

- ACCT-CODE-PROMPT-DELAY, ACCT-CODE-PROMPT-TIMEOUT, ACCT-CODE-PROMPT-TONE.
- AUTH-CODE-PROMPT-DELAY, AUTH-CODE-PROMPT-TIMEOUT, AUTH-CODE-PROMPT-TONE.

For general COS provisioning, see the Class of Service (COS) provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

For more details about IVR interactions, see Chapter 6, "Interactive Voice Response Functions."

To provision IVR support for features that use the IVR functionality, see the applicable feature provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

ANI Screening on Incoming Calls

Automatic number identification (ANI) screening is a service commonly found in Tandem switches, and is used for long-distance access service. The ANI is the number of the calling party (NDC + EC + DN). Full or partial ANIs can be specified for screening. The ANI screening feature validates the ANI on incoming trunk group (TG) calls from the public switched telephone network (PSTN) before routing. All ANIs to be screened are stored in the Feature Server database. If an ANI is not available, or does not appear in the Feature Server ANI table, the call is considered as a casual call. The TG restrictions are checked to see if casual calls are allowed. If casual calls are not allowed, the call is denied and routed to an announcement. If the ANI exists in the table, the ANI status is checked next. The ANI status can either be allowed or blocked. If the status is blocked, the call is blocked and routed to an announcement. COS can also be applied on an ANI basis.

When an incoming call is received over a Trunk Group marked for ANI Screening, the Cisco BTS 10200 screens the incoming number against a provisioned list of ANIs in the ANI-SCREENING table. The ANI-SCREENING-PROFILE-ID provisioned in the Trunk Group table and the received ANI is used to index the ANI-SCREENING table. To provision ANI screening on incoming calls, see the *Cisco BTS 10200 Softswitch SIP Guide*. For more information on the ANI screening table, see the *Cisco BTS 10200 Softswitch CLI Database*.

Temporary Disconnect Treatment

The service provider can designate a subscriber as temporarily disconnected (for example, for nonpayment of bills) and use COS screening to limit the types of calls the subscriber is allowed to make. For example, a special set of COS restrictions can allow temporarily-disconnected subscribers to call only the repair number.

For subscribers with STATUS=TEMP-DISCONNECTED in the Subscriber table, the system ignores the COS restriction ID for the subscriber (in the Subscriber Profile table), and instead uses the TEMP-DISC-COS-RESTRICT-ID token in the Point of Presence (POP) table.

Note For a full description, see the "Temporarily Disconnected Subscriber Status and Soft Dial Tone" section in Chapter 3, "Subscriber Features."

COS Restriction Priorities

For any call, it is possible that a combination of call categories are applicable. Under these conditions, the system performs Black White List screening first. If the call passes (is allowed from) Black White List screening, then the system applies COS restriction screening.

COS restrictions can be assigned to any ANI, authorization code, trunk group, or POTS subscriber. When multiple COS restrictions apply to a trunk call, the system uses the order of precedence as follows:

1. Use the COS assigned to ANI if found in the ANI screening table.
2. If not found in ANI screening table, use the COS assigned to the TG.
3. If an authorization code is required, then use the COS assigned to authorization code.

When a call is blocked due to COS screening, the call event shows which type of screening blocked the call. The service provider can provision the treatment of blocked calls, and can include, for example, playing an announcement or sending a cause code to the originator.

High-Level Flowchart of COS Screening Process

Figure 4-1 and Figure 4-2 show a high-level flowchart of the COS screening process. The flowchart is split into two parts (two drawings) for easier viewing.

Figure 4-1 COS Screening Process (Part 1)

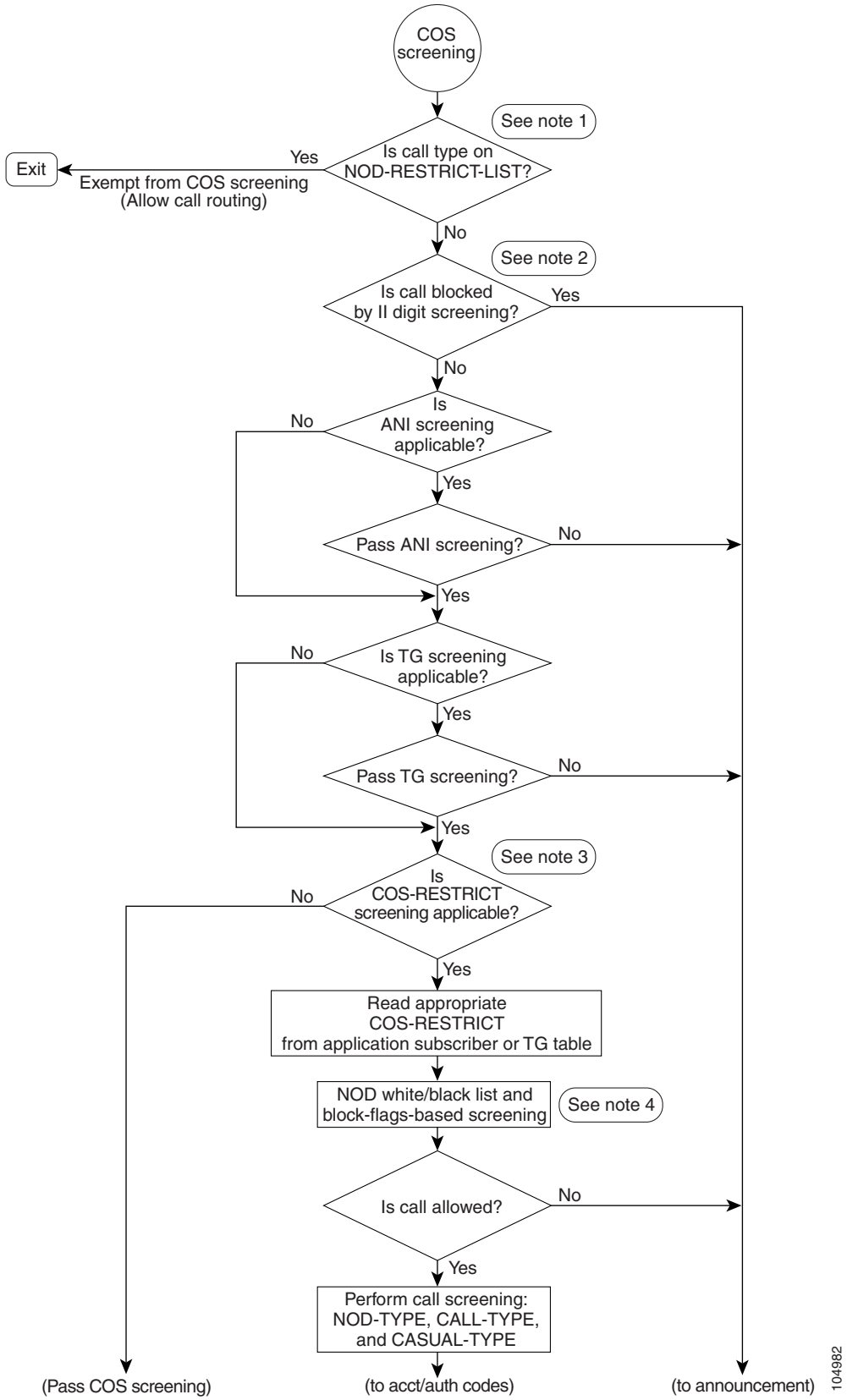
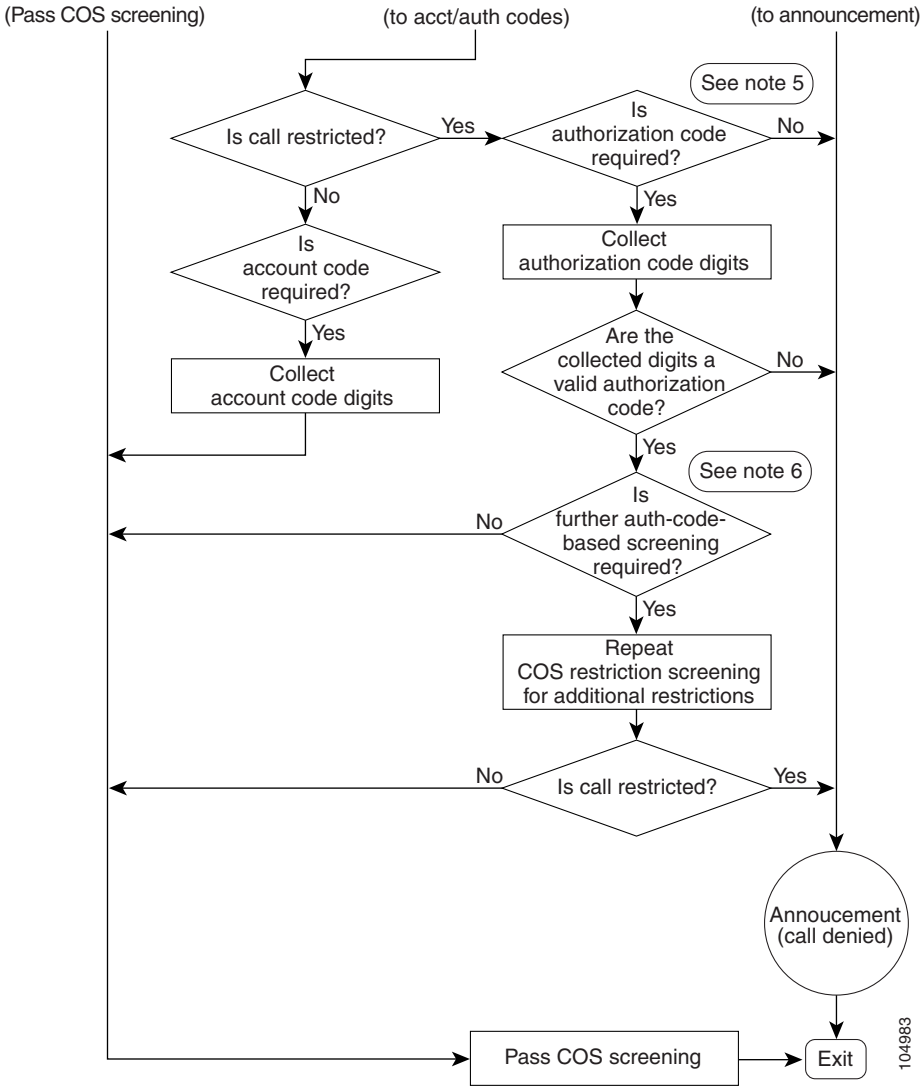


Figure 4-2 COS Screening Process (Part 2)



Notes for Figure 4-1 and Figure 4-2:

1. Call types on the NOD-RESTRICT-LIST are exempt from COS screening.
2. II = 24 and 25 are reserved for translated toll-free calls and are exempt from II screening.
3. COS-RESTRICT screening is applicable if either the subscriber or the TG has an associated COS-RESTRICT-ID.
4. Block flags are as follows:
   - BLOCK-900
   - BLOCK-976
   - BLOCK-DA
   - BLOCK-INFO
   - BLOCK-TW

- BLOCK-INTL
- BLOCK-NANP-OPER-ASSIST
- BLOCK-INTL-OPER-ASSIST

Note NOD-WB-LIST has a higher precedence that the block flags during screening.

5. The initial check of the authorization code is based on the provisioned value for AUTH-CODE-ALLOW in the applicable COS-RESTRICT table.
6. The additional check of authorization code is based on the COS-RESTRICT-ID provisioned in the applicable AUTH-CODE table.

Outgoing Call Barring (OCB)

This section describes the BTS 10200 support for the outgoing call barring (OCB) feature. The OCB feature allows an individual subscriber or business group administrator to restrict certain types of outgoing calls. Once OCB is provisioned and activated on a calling line, the OCB restrictions are transparently invoked on all outgoing calls.

The BTS 10200 support for the OCB feature complies with the International Telecommunications Union standard *ITU-T I.255.5, Outgoing Call Barring*.

The class of service (COS) feature is an optional functionality (subset) of OCB. The service provider can provision the COS feature by itself, without the OCB feature. The details are discussed later in this section.

Certain types of calls are exempt from both COS and OCB restrictions. See this information in the "COS Functional Description" section on page 4-2.

This section covers the following topics:

- OCB Highlights
- OCB Subscription and Provisioning
- OCB Activation and User Options
- OCB Deactivation
- OCB Interrogation
- OCB Invocation and Screening
- OCB Lockout Behavior
- How to Coordinate OCB and COS Provisioning
- OCB Feature Interactions
- Limitations and Restrictions
- Additional Documents with OCB Information

OCB Highlights

The following list highlights some of the major functions and behaviors for the OCB feature:

- The range of K-values (call-barring levels) is 1 through 9, and the service provider can provision each of the 9 values for specific call types. The default K-values are K=1 (all calls), K=2 (domestic long distance and international), and K=3 (international). These values are automatically enabled for the handset user when the OCB feature is provisioned by the service provider.
- K-values can be mapped to call-types at the POP or at the office level. If K-values are not mapped at the POP level, the software checks to see if they are mapped at the office level. If K-values are not provisioned at either the POP or office level, OCB defaults to the hard-coded mapping of the three K-values as in Release 3.2. K-value mapping need not be configured per subscriber.
- Only one K-value can be active at any time on a specific subscriber line.
- The service provider can provision three deactivation options for the handset user, including the option to deactivate only if the user enters a currently-active K-value. By default, the system deactivates OCB without checking the K-value the user enters.
- If the user attempts to reactivate OCB to the same K-value that is currently active, the system treats the attempt as a new attempt, and provides the same success announcement as for the previous activation. If the user attempts to activate OCB to a different K-value than is currently activated, the system plays the appropriate announcement.
- The PIN length is provisioned by the service provider and cannot be provisioned by the user via the handset, and cannot be changed by the user. The initial PIN setup can be performed either by the service provider, or can be provisioned for the user to set up using the handset. However, the initial PIN cannot be changed by the handset user.
- If a user forgets the original password, the service provider (after proper authorization) can reset the password.

OCB Subscription and Provisioning

The service provider sets up OCB service at the request of the subscriber. There are a number of service provider provisionable parameters that affect the behavior of the feature on the subscriber line:

- Vertical service code (VSC)—ASCII strings that the user must enter to access OCB activation, deactivation, and interrogation options. The recommended values are *54*, #54* and *#54# as used in the examples below. However, VSCs are not preprovisioned in the system. The service provider can provision these values with any valid unique ASCII string up to five characters long.

  Note The valid formats for VSC ASCII strings are listed in the VSC table specification in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*. The preprovisioned VSC values are listed in the Vertical Service Code appendix of the same document.

- Private identification number (PIN)—A digit string that the user must enter for authorization to set OCB activation and deactivation options from his or her local phone.

  Initially, the service provider or the user establishes a PIN for the user. Thereafter, the user cannot modify the PIN.

- PIN length (PIN-LEN)—The number of digits required for a valid PIN (can be provisioned as 1 to 8 digits).

  The PIN and PIN-LEN can be provisioned by the service provider.

The PIN and PIN-LEN cannot be provisioned or changed by a user via the handset if the OCB-PROFILE has not been provisioned at either the point-of-presence (POP) or at the office level. However, if the OCB-PROFILE has been provisioned and the FREE_SELECT_PIN token has been set to Y (Yes), a subscriber can free-select and register a PIN using a handset at activation if a PIN has not already been assigned and registered.

- Allowed activation/deactivation attempts and lockout parameters—OCB can be provisioned to limit the number of times that a user can enter an incorrect PIN within a specified time. If the limit is exceeded, the system ignores further activation and deactivation attempts for a provisionable length of time (lockout period).

OCB Activation and User Options

OCB activation (OCBA) allows a user to activate OCB and select various call barring options on the handset (local phone). A user does this by dialing *54*K-VALUE<PIN># (the trailing # is optional to signify the end of the entry). The parameters are defined as follows:

- *54* is the VSC the user enters on the handset to access the OCBA feature.

  K-VALUE is the parameter that determines the type of outgoing calls to be barred. OCB can enable K-values up to 9 levels. The K-Value can be mapped to a special mapping table, the OCB-K-Value table.

Note Emergency calls (calls with call type set to EMG) are not barred, regardless of the specified K-value.

- <PIN> is the assigned private digit string that the user must enter. A success announcement is given on a successful activation, and an error announcement, indicating the type of error, is given if activation is unsuccessful.

Note The K-VALUE can be changed when the OCB feature is active if the subscriber performs another activation and enters a different value for the K-VALUE token. The new K value overwrites the preceding K value.

If a user enters an incorrect PIN repeatedly in a specified time period, the system can lock out further activation or deactivation attempts, as described in the "OCB Subscription and Provisioning" section on page 4-15.

The following user actions are invalid, and the system provides an appropriate error announcement:

- The user enters a value for K-VALUE that is not in the range 1 through MAX-K-VALUES (as specified in the OCB-PROFILE table).

  If a subscriber attempts an activation and specifies a K-VALUE that is not in the range established by the provisioned MAX-K-VALUE token, the subscriber receives an error announcement. If the MAX-K-VALUES token is not provisioned in the OCB-PROFILE table at either the POP or BTS 10200, by default, the valid K-VALUE range is 1 through 3.

  The POP table is checked first for the MAX-K-VALUE and then the office level (call agent configuration table). If the token is not provisioned in either table, OCB defaults to the behavior established in the initial release of OCB in Cisco BTS 10200 Release 3.2.

- The user is not provisioned for the OCB feature.
- The user enters an incorrect PIN.

OCB Deactivation

The Enhanced OCB feature supports three options for OCB deactivation. An option is specified by provisioning the DEACTIVATION-OPTION token in the OCB-PROFILE table.

NO-K-VALUE Option

To select the NO_K_VALUE deactivation option, the subscriber enters <VSC><PIN> without entering a K-VALUE.

K-VALUE-NO-MATCH Option

The K-VALUE-NO-MATCH deactivation option enables a user to deactivate all OCB on the handset. The user does this by dialing #54*K-VALUE<PIN>#. The parameters are defined as follows:

- #54* is the VSC the user enters on the handset to access the OCBD feature
- K-VALUE must be entered as a value from 1 through MAX-K-VALUES. However, the actual value is ignored during processing.
- <PIN> is the same as for OCBA.

  If the K-VALUE token is not provisioned in the OCB-K-VALUE table at either the POP or softswitch, by default, the K-value range is 1 through 3.

K-VALUE-MATCH Option

The K-VALUE-MATCH deactivation option requires the subscriber to enter a K-VALUE that matches the K-VALUE provisioned for the subscriber. If the subscriber enters a K-VALUE that does not match the value provisioned for K-VALUE, the subscriber receives an error announcement.

Additional Deactivation Details

A success announcement is given on a successful deactivation, and an error announcement, indicating the type of error, is given if deactivation is unsuccessful.

Refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for provisioning details.

If a user enters an incorrect PIN repeatedly in a specified time period, the system can lock out further activation or deactivation attempts, as described in the "OCB Subscription and Provisioning" section on page 4-15.

OCB Interrogation

OCB interrogation allows a user to check the level of outgoing call restrictions on his or her local phone. The dial string for OCB Interrogation is *#54#. No PIN is required to use this feature. The system provides an appropriate announcement to the user.

OCB Invocation and Screening

For a calling party that is subscribed to OCB, and has activated the feature, the feature is invoked for every call made after the called party digits are dialed. There is no user driven invocation method involved for the feature. Once provisioned for a calling party, and activated on the calling party's line, the invocation is handled automatically by the BTS 10200.

OCB Lockout Behavior

The LOCK-OUT, TIME-OUT, and FAIL-CNT tokens in the OCB-PROFILE and FEATURE tables are intended to prevent unauthorized changes or bypassing of OCB screening. If a user repeatedly enters the PIN incorrectly on the handset, the system can lock the line against both OCBA and OCBD.

- If the FAIL-CNT (fail count), LOCK-OUT, and TIME-OUT tokens are provisioned in the OCB-PROFILE table, OCB lockout behaves according to those specifications.
- If the OCB-PROFILE table is not provisioned, OCB lockout behaves according to the provisioning of the LOCK-OUT, TIME-OUT, and FAIL-CNT tokens in the FEATURE table.

The tokens control the lockout behavior as described in Table 4-1.

Tip Note that there is no service lockout when either the TIME-OUT or FAIL-CNT token is set to zero.

Table 4-1 OCB Lockout Behavior

OCB Tokens in Feature Table			Lockout Behavior Due to OCBA/OCBD Misuse
LOCK-OUT	TO	FAIL-CNT	
n/a	n/a	0	No service lockout
n/a	0	n/a	No service lockout
0	1 or greater	1 or greater	OCBA and OCBD are locked out indefinitely after the user misuses the OCBA/OCBD feature <FAIL-CNT> times in <TO> minutes
1 or greater	1 or greater	1 or greater	OCBA and OCBD are locked out for <LOCK-OUT> minutes after the user misuses the OCBA/OCBD feature <FAIL-CNT> times in <TO> minutes

How to Coordinate OCB and COS Provisioning

Typically, service providers in North America provide the COS feature set, but not the OCB feature set, to their customers. In the rest of the world, service providers typically provide OCB. On the BTS 10200, the black/white list functionality of OCB is contained in the COS module. Therefore, to provide black/white-list functionality with OCB, you must:

- Assign the OCB feature and provision the desired OCB options for each subscriber.
- Provision the desired black/white-list COS restrictions for each OCB subscriber, and assign a COS-RESTRICT-ID for the subscriber. This ensures that the black and white list restrictions are in effect, even if the user deactivates OCB. It is optional to include the COS feature in the Subscriber Service Profile table.

Table 4-2 summarizes how to coordinate provisioning options for COS and OCB.

Table 4-2 Coordination of Provisioning Options Between COS and OCB Features

Feature Included (1) or Excluded (0) in the Service Provisioned for the Subscriber		COS-RESTRICT-ID Included (1) or Excluded (0) in the Subscriber Table for the Subscriber	Features Delivered by the System [1] [2]	How the System Reports Billing Data
OCB Feature	COS Feature			
0	0	0	No restrictions on outgoing calls.	n/a
0	0	1	No restrictions on outgoing calls.	n/a
0	1	0	No restrictions on outgoing calls.	n/a
0	1	1	Full COS functionality. No OCB.	COS
1	0	0	OCB, but without black/white list. No COS.	OCB
1	0	1	OCB with black/white list. To the extent that COS-RESTRICT is configured, additional COS features apply to the subscriber. In this case, OCB treatment takes precedence over COS treatment.	OCB
1	1	0	OCB, but without black/white list. No COS.	OCB
1	1	1	OCB with black/white list. To the extent that COS-RESTRICT is configured, additional COS features apply to the subscriber. In this case, OCB treatment takes precedence over COS treatment.	OCB

1. This description assumes that OCB (if provisioned for the subscriber) has been activated by the subscriber.
2. For details of the COS feature, see the "Class of Service Restrictions" section on page 4-1.

OCB Feature Interactions

The section describes the interactions of OCB with other features.

OCB Interaction with Call Forwarding

The interaction of OCB and call forwarding features depends upon the sequence in which they are activated.

Note In this section, "CFx" refers to any of the call forwarding features, CFU, CFB, CFNA, or call forwarding combined (CFC).

- If OCB is activated prior to CFx activation—OCB screening is performed on each DN the user enters when attempting to activate CFx. Successful CFx activation depends on the existing OCB K-VALUE and the forward-to DN:
  - If the existing OCB K-VALUE is set to block calls to the forward-to DN, then the system does not allow CFx activation. The user receives an error announcement.
  - If the OCB K-VALUE allows calls to this DN, then the CFx activation process continues. Once the CFx activation attempt to a specific DN is accepted by the system, it is applicable permanently regardless of any future OCB K-VALUE changes. That is, future changes to the OCB K-VALUE have no effect on CFx invocation. CFx to this DN can be deactivated by the user in the normal manner (#XX#).
- If CFx is activated prior to OCB activation—The user can activate the OCB feature, or change the OCB K-VALUE, regardless of the existing CFx feature. However, invocation of OCB depends upon the type of call:
  - User-dialed calls—User-dialed calls can be blocked by OCB (depending on the K-VALUE).
  - Forwarded calls—CFx remains active as originally set up by the user, therefore, calls forwarded by the CFx feature *are not* blocked using OCB screening.

OCB Interaction with COS Restriction

If the OCB is assigned and active on the subscriber line, the COS-RESTRICT-ID is provisioned for the subscriber, and the black/white-list functionality is also provisioned, the subscriber will receive OCB treatment including black/white-list functionality. The system will apply all provisioned COS features to the subscriber, but OCB treatment takes precedence over COS treatment. For more information on coordinating the provisionable features of COS and OCB, see Table 4-2.

Note The service provider can provision an exception list to override COS and OCB screening on certain types of calls. See the "Exemptions from COS and OCB Restrictions" section on page 4-2.

Limitations and Restrictions

This section provides information on limitations and restrictions that apply to certain OCB options.

Limitations On Reporting of Traffic Counters

The BTS 10200 OCB does not support the following traffic counters when it uses the OCB-Profile to block calls:

- POTS_OCB_LOCAL_BLOCKED
- POTS_OCB_NATL_BLOCKED
- POTS_OCB_INTL_BLOCKED

Special Call Types

Emergency calls (calls with call-type=EMG) are never subject to COS and OCB screening. The system always exempts emergency calls from COS and OCB screening without considering any provisioned parameters. You can provision AMBULANCE, FIRE, and POLICE as subtypes of EMG in the Destination table. If provisioned as subtypes of EMG, these types are given the same treatment as EMG.

SIP Subscribers

If the service provider sets NANP_DIAL_PLAN=”Y” in the dial plan for a SIP subscriber, the OCB feature will not operate properly.

Additional Documents with OCB Information

This section describes the OCB feature and the impact of certain provisionable parameters. It should be used in conjunction with the OCB information in the following documents:

For information on all of the CLI parameters, see the *Cisco BTS 10200 Softswitch Provisioning Guide.*

For the sequence of commands used to provision this feature, see the OCB provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

For a list of cause codes and announcements, see the *Cisco BTS 10200 Softswitch Provisioning Guide*.

For a list of traffic measurements (counters), see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

For billing procedures and data, see the *Cisco BTS 10200 Softswitch Billing Guide*.

CHAPTER 5

Feature Interactions

Revised: March 24, 2011, OL-12606-21

This chapter describes the interactions among the various features offered by the Cisco BTS 10200 Softswitch. It includes the following topics:

- Overview of Features and Services, page 5-2
- Creation of Features and Services, page 5-2
- Trigger Detection Points, Trigger IDs, and Call States, page 5-5
- Feature Precedence, page 5-7
- Feature Inhibition, page 5-9
- Special Interaction Scenarios, page 5-13
- Examples of Interactions, page 5-14

Service providers define the features and services for their system, and assign these services to subscribers. A service is a collection of features. Each feature has static information, stored in the feature table, regarding triggers, feature defaults, associated features, and vertical service codes. When a service is created, the system automatically maps the service with the triggers. The system uses internal information about triggers and trigger detection points (TDPs), based on the ITU-T CS-2 call model, to process features during a call. The system has internal information to handle features that interact with other features at specific detection points. The system also handles features that are inhibited when certain other features are already invoked on the subscriber line.

Note See Chapter 1, "Network Features" and Chapter 3, "Subscriber Features" for detailed descriptions of individual features.

Caution Some features involve the use of other network elements (NEs) deployed in the service provider network, for example, gateways, media servers, announcement servers, eMTAs, and SIP phones. See the Component Interoperability section of the *Release Notes* for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the Cisco BTS 10200 Softswitch Release 5.0 software. Earlier or later releases of platform software might be interoperable and it might be possible to use other functions on these platforms. That list certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the Cisco BTS 10200 Softswitch.

Overview of Features and Services

Service providers use command-line interface (CLI) commands to provision the features and services for their system. The feature table contains all the static information for a feature, such as:

- Trigger detection point (TDP)
- Trigger ID (TID)
- Trigger type
- Vertical service code, if any
- Feature Server
- Feature defaults
- Associated features, if any (for example, CFU_ACT and CFU_DEACT can be associated with CFU)

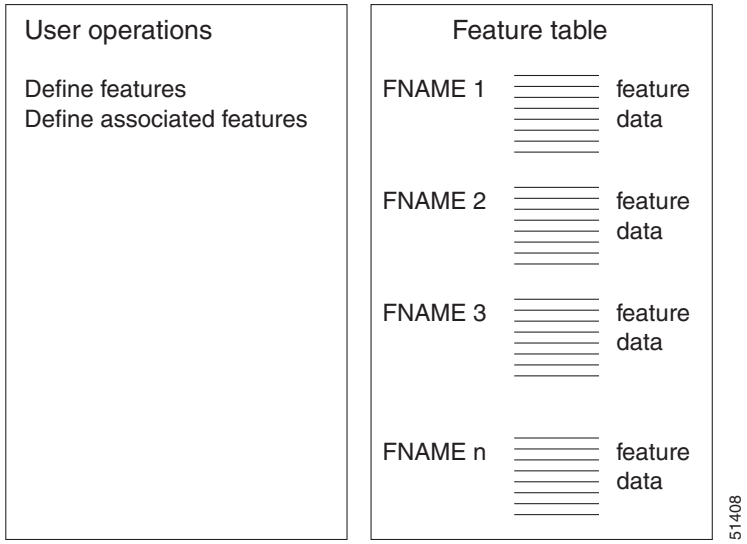
A service is a collection of one or more features (up to 10 features per service). Each service is identified by a unique service ID numeric value. Each feature within a service may have one or more triggers. When a service is created, the system automatically registers the triggers. During call processing, the services are triggered based on TDP and TID. The Cisco BTS 10200 Softswitch supports provisioning of up to 50 services per subscriber.

Note Limitation—If services are defined (by the service provider) such that they share the same TDP-TID pair, the Cisco BTS 10200 Softswitch supports a maximum of 10 services for that TDP-TID pair.

Creation of Features and Services

Figure 5-1 through Figure 5-3 show the process of creating features, assembling features into services, and assigning services to individual subscribers (or subscriber groups). The provisioning operations listed in these figures are performed using CLI commands. Feature provisioning steps are provided in the *Cisco BTS 10200 Softswitch Provisioning Guide*. Detailed reference information on commands and parameters (tokens) is provided in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

Figure 5-1 Defining Features and Associated Features



Note Associated features, such as CFU_ACT and CFU_DEACT, must be defined first, and then they can be linked (associated) with the main feature (CFU in this case).

Figure 5-2 Assigning Features to Services

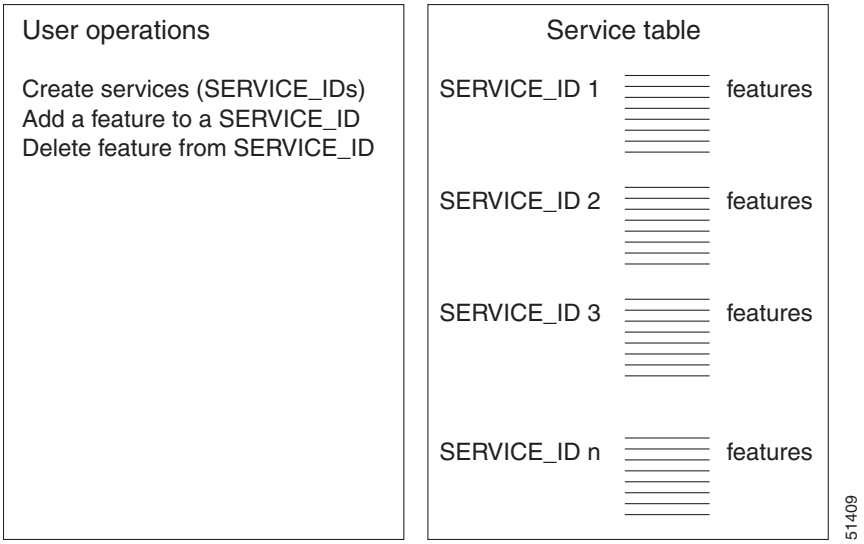
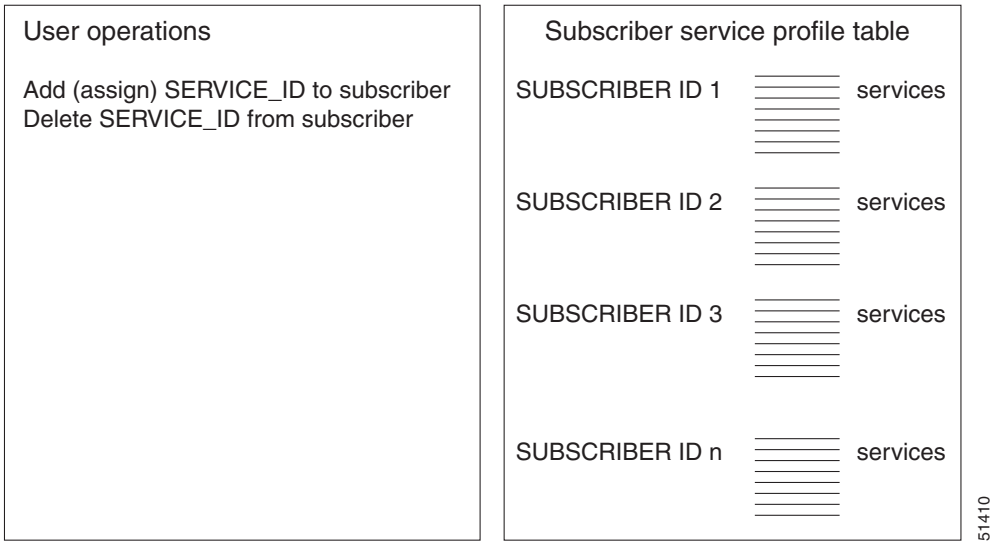


Figure 5-3 Assigning Services to Subscribers



Trigger Detection Points, Trigger IDs, and Call States

The call states and triggers for the Cisco BTS 10200 Softswitch are illustrated in Figure 5-4 and Figure 5-5.

Note The basic call module of the Cisco BTS 10200 Softswitch contains the triggers specified in the standard ITU-T CS-2 call model, as well as several additional triggers.

For illustration purposes, Table 5-1 lists several examples of TDPs and TIDs for some features.

Note For a complete list of TDPs and TIDs for all features, see the *Cisco BTS 10200 Softswitch CLI Database* and use the **show feature** command.

Table 5-1 Examples of Service Triggers (Partial List, for Illustration Purposes)

Feature	Description	Trigger Detection Point	Trigger ID
911	Emergency service	COLLECTED_INFORMATION	911_TRIGGER
CFU	Call forwarding unconditional	TERMINATION_ATTEMPT_ AUTHORIZED	TERMINATION_ATTEMPT_ AUTHORIZED
CFUA	CFU activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CFUD	CFU deactivation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CHD	Call hold	O_MID_CALL	O_SWITCH_HOOK_FLASH_ IMMEDIATE
		T_MID_CALL	T_SWITCH_HOOK_FLASH_ IMMEDIATE
CIDCW	Caller ID with call waiting	T_BUSY	T_BUSY
CNAM	Calling name delivery	FACITLITY_SELECTED_AND_ AVAILABLE	TERMINATION_RESOURCE_ AVAILABLE
CNDB	CND blocking (toggles the privacy indicator)	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
COS	Class of service screening	COLLECTED_INFORMATION	COS_TRIGGER
SCA	Selective call acceptance	TERMINATION_ATTEMPT_ AUTHORIZED	TERMINATION_ATTEMPT_ AUTHORIZED
SCA_ACT	SCA activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
		T_ANSWER	T_ANSWER

Figure 5-4 BTS 10200 Originating Call States and Triggers

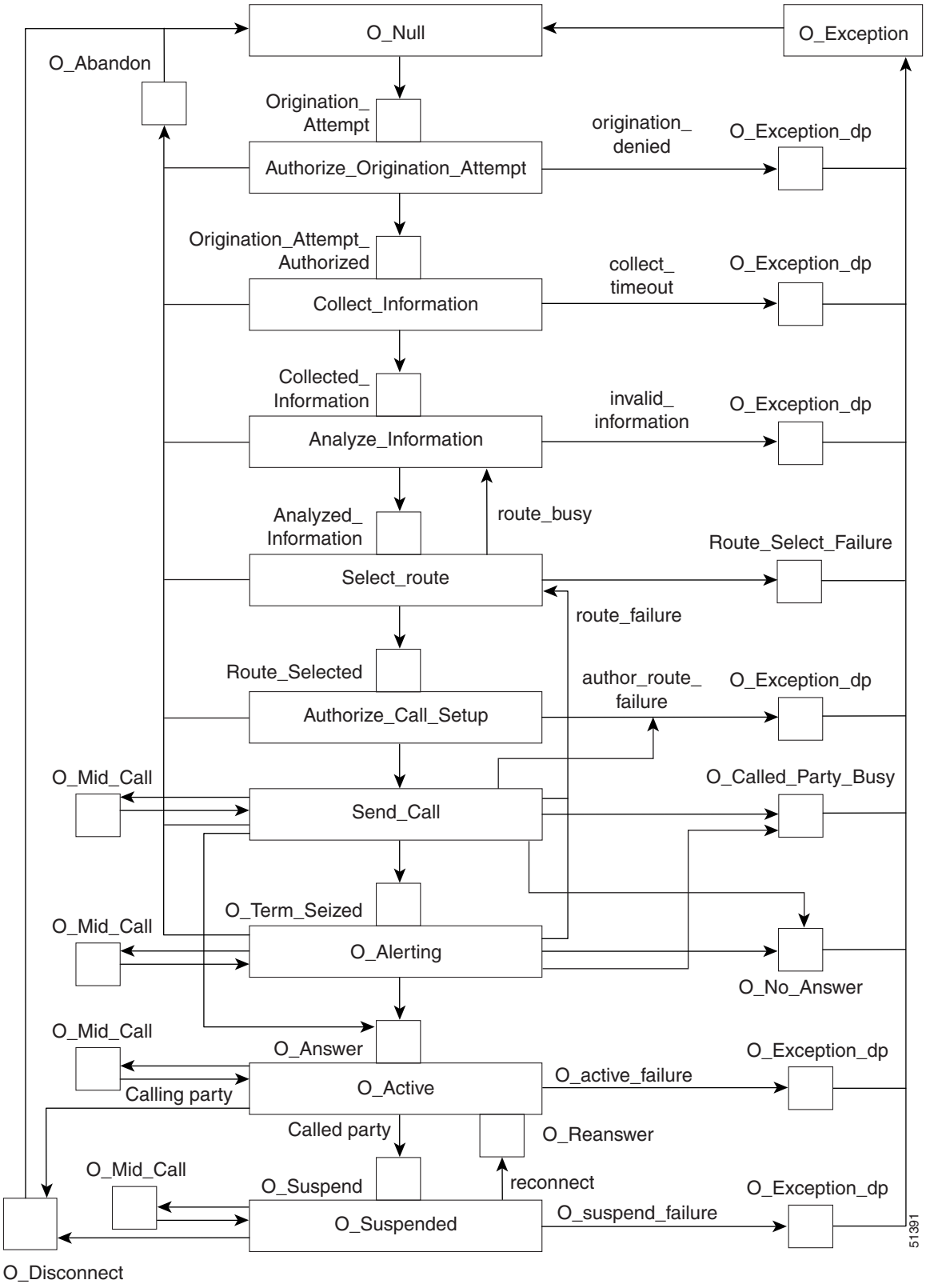
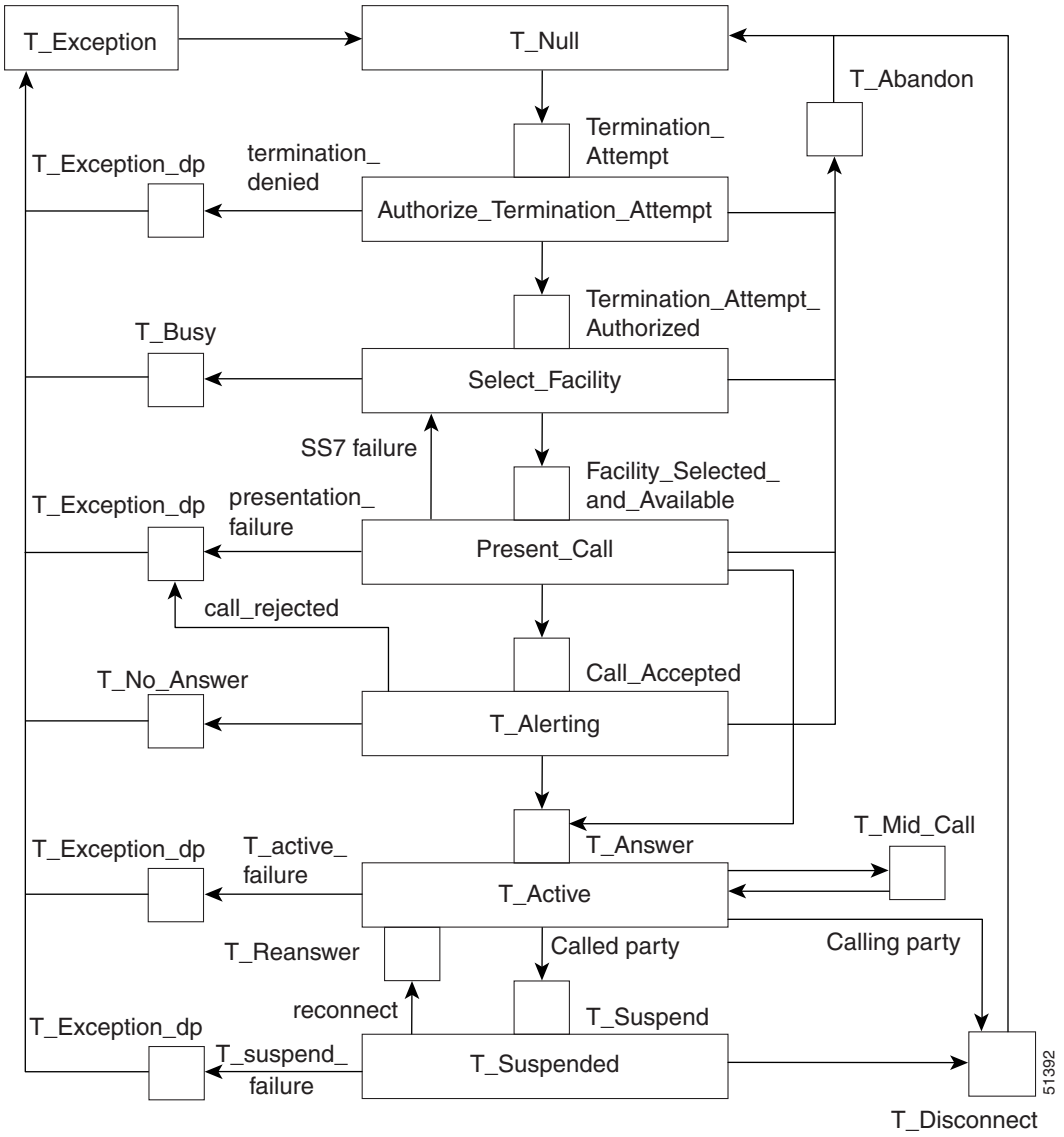


Figure 5-5 BTS 10200 Terminating Call States and Triggers



Feature Precedence

If the call processing function in the CA detects a TDP, it sends a trigger, if applicable, to the appropriate Feature Server (FS). After receiving the trigger, the FS controls the call as needed. With multiple features assigned to a single service package, it is possible for more than one feature to trigger at the same TDP. When that occurs, the Cisco BTS 10200 Softswitch uses the feature precedence table (Table 5-2), along with the subscription information of the subscriber, to determine which feature to provide. If multiple features are included in a service package (as they often are), it is important for the service provider to be able to identify to their subscribers which feature takes precedence at a particular TDP. The TDPs for each feature, and the precedence conditions for specific feature pairs, are defined in the system and cannot be changed. The precedence functionality is implemented in accordance with the LSSGR specification.

Note For a list of triggers for services that contain multiple features, see the *Cisco BTS 10200 Softswitch CLI Database* and use the **show service-trigger** command.

Tip As shown in Figure 5-4 and Figure 5-5, a call reaches TDPs in a specified sequence consistent with the CS-2 call model. A feature triggered at an earlier TDP is ***not*** said to have precedence over a feature triggered at a later TDP. Precedence refers to a scenario in which two features occur ***at the same TDP***, and the Cisco BTS 10200 Softswitch uses internally programmed rules to determine which feature takes precedence at that TDP.

Table 5-2 Feature Precedence

No.	Trigger Detection Points (TDP)	Precedence
1	TERMINATION_ ATTEMPT_AUTHORIZED	• SCR has priority over: SCF DRCW SCA ACR CFU DND MDN DACWI • ISFG has priority over CFU • SCF has priority over: DRCW SCA ACR CFU DND MDN DACWI • DRCW has priority over: ACR [1] CFU [1] DND MDN DACWI • SCA has priority over: ACR CFU DND MDN DACWI DRCW • ACR has priority over: CFU [1] DND MDN DACWI • CFU has priority over: DND MDN DACWI • DND has priority over: MDN DACWI • MDN has priority over: DACWI

Table 5-2 Feature Precedence (continued)

No.	Trigger Detection Points (TDP)	Precedence
2	FACILITY_SELECTED _AND_AVAILABLE	• CNAM has priority over CND (CNAM includes CND. If a subscriber has both features, CNAM is provided.)
3	T_BUSY	• CIDCW has priority over: CW CFB • CW has priority over CFB
4	O_ATTEMPT_AUTHORIZED	• HOTLINE has priority over WARMLINE
5	COLLECTED_INFORMATION	• CDP and VSC are independent features, with different triggers • CDP has priority over COS • Call agent does not report COS trigger for VSC dialed
6	O_MIDCALL and T_MIDCALL	• CT has priority over: TWC TWCD

1. If all three features (DRCW, ACR, and CFU) are assigned to a subscriber, CFU takes precedence over ACR and DRCW.

Feature Inhibition

Feature inhibition is defined as an interaction where the subscriber's current feature status inhibits other features from being provided. The inhibition functionality is implemented in accordance with the LSSGR specification. This table is preset in the system and cannot be modified. Table 5-3 shows how features are inhibited by various other features.

Tip If a call is released at a particular TDP, the later TDPs will not be reached, and the features associated with those later TDPs will not occur. This is a direct result of the TDP sequencing, and is not defined as inhibition. Feature inhibition occurs when a trigger is reached, but one of the features associated with the TDP has been inhibited by a feature that occurred at an earlier TDP.

Note MDC refers to midcall, which is a function activated when the user presses the Flash button or hookswitch during a call. In Table 5-3, MDC is treated as an internal feature, with the following meaning:

Certain features inhibit MDC. This means that when one of those features is invoked, the Cisco BTS 10200 Softswitch ignores the Flash and hookswitch functions.

MDC inhibits several features. This means that those features cannot be supplied to the user after the user presses the Flash button or hookswitch.

Table 5-3 Feature Inhibition

Feature	Feature State	Inhibited Features	Remarks
911	Invoked	CIDCW COS CW MDC	
ACR	Deactivated	ACR	
BLV	Invoked	ACR CFB CFNA CFU CIDCW CNAM CND COS CT CW DND DRCW ISFG MDC MDN OSFG RACF SCA SCF SCR TWC USTWC	
CCW	Invoked	CIDCW, COT, CW	
CFU	Invoked	CFU	Applicable only if MCF flag for CFU in the feature table is set to no (N).
	Deactivated	CFU	
CFB	Invoked	CFB	Applicable only if MCF flag for CFB in the feature table is set to no (N).
	Deactivated	CFB	
CFNA	Invoked	CFNA	Applicable only if MCF flag for CFNA in the feature table is set to no (N).
	Deactivated	CFNA	

Table 5-3 Feature Inhibition (continued)

Feature	Feature State	Inhibited Features	Remarks
CHD	Invoked	911 AC, AC_ACT, AC_DEACT AR, AR_ACT, AR_DEACT CBLK CFBVA, CFBVD CFNAVA, CFNAVD CFUA, CFUD CIDCW CNDB COT CPRK, CPRK_RET CW DPN DPU	
CIDCW	Invoked	CIDCW CNAM CND CW MDC TWC	
CNDB	Invoked	CNDB	
COT	Invoked	CIDCW CT CW MDC TWC USTWC	
CT	Invoked	AC, AC_ACT, AC_DEACT AR, AR_ACT, AR_DEACT CBLK CIDCW COT CPRK_RET CT CW MDC TWC	
CW	Invoked	CIDCW CNAM CND CW MDC TWC	
DND	Deactivated	DND	
DRCW	Deactivated	DRCW	

Table 5-3 Feature Inhibition (continued)

Feature	Feature State	Inhibited Features	Remarks
DRCW_ACT	Invoked	CHD CIDCW CT CW MDC TWC	
HOTLINE	Assigned (provisioned by service provider)	CT MDC TWC USTWC VSC based features	
MDC	Invoked	AC, AC_ACT, AC_DEACT ACR_ACT, ACR_DEACT AR, AR_ACT, AR_DEACT CBLK CFBVA, CFBVD CFUA, CFUD CIDCW CNDB COT CPRK_RET CW DND_ACT, DND_DEACT DPN DPU MDC SC1D_ACT, SC2D_ACT	
SC1D_ACT	Invoked	CFUA	
SC2D_ACT	Invoked	CFUA	
SCA	Activated	ACR, DND	
	Deactivated	SCA	
SCA_ACT	Invoked	CHD CIDCW CT CW MDC TWC	
SCF	Deactivated	SCF	
SCF_ACT	Invoked	CHD CIDCW CT CW MDC TWC	
SCR	Deactivated	SCR	

Table 5-3 Feature Inhibition (continued)

Feature	Feature State	Inhibited Features	Remarks
SCR_ACT	Invoked	CHD CIDCW CT CW MDC TWC	
TWC	Invoked	AC, AC_ACT, AC_DEACT AR, AR_ACT, AR_DEACT CBLK CIDCW COT CPRK_RET CT CW MDC TWC	
WARMLINE	Assigned (provisioned by service provider)	CT MDC TWC USTWC VSC based features	

Special Interaction Scenarios

This section describes additional interaction scenarios.

DND and CFB Interaction

If a called party (subscriber) is assigned both the DND and CFB features, and has activated them, an incoming call will be forwarded to the CFB forward-to DN whether the called party is busy or not.

CHD, CFNA, and CW Interaction for Centrex Subscriber

There is an interaction when a Centrex subscriber has all three of the following features assigned and active:

1. Call hold—CHD.
2. Call waiting—CW or CIDCW or both.
3. Call forwarding on no answer—CFNA, VM (or VMA), or any combination of these.

(Prior to Release 5.0 Maintenance Release 1.1) In this case, the system does not invoke forwarding for any incoming calls. If the subscriber wants to have the call-waiting features (CW or CIDCW) and call-forwarding features (CFNA, VM, or VMA) active simultaneously, the service provider should not assign the CHD feature to that subscriber.

(Release 5.0 MR1.1 and later) The system behavior is illustrated in the following example. In this example, CFNA is assigned and active on subscriber (A) along with CHD and CW.

- A and B are on an active call.
- C calls A.
- A hears the CW tone. (C hears ringback.)
- If A presses the **Flash** button or **hookswitch**, B is put on hold and A hears a dial tone.
- If A dials *52, A is connected to C.
- If A ignores the CW tone, C continues to hear ringback until the CFNA timer expires, then the call from C is forwarded per CFNA.

Examples of Interactions

Feature interaction examples are presented in this section for the following scenarios:

- Three-way calling
- Call waiting
- Calling number delivery

Three-Way Call Interaction

The following interactions pertain to three-way calling (TWC):

- TWC can interact with itself. Given three parties involved in a call, any party with the TWC feature who has not already added can flash and add on another party. In other words, TWC can be recursively used to join more than three parties.
- A customer who has initiated TWC cannot initiate TWC again while in a TWC conference call.
- The use of TWC does not restrict the call waiting capabilities of the customers who did not initiate TWC.
- The initiator of TWC does not receive CW calls or the CW tone while in a TWC mode or while a party is on hold.
- When a line that is not the initiator of TWC receives a CW call, a flash is not interpreted as a request for TWC (that is, CW takes precedence over TWC in this case).
- TWC can be used to disable CW during an existing conversation.
- When CW is in effect, it takes precedence over TWC. When CW is disabled, TWC treatment is given when the customer flashes.
- If a customer activates cancel call waiting (CCW) and then originates TWC, CW remains disabled until all connections are torn down. If either of the noncontrolling parties of TWC disconnect (or are disconnected by the controller), CW remains disabled for the remaining two-way connection.
- If the initiator of TWC hangs up with a party on hold, the initiator will be rung back and connected to the held party on answer. If the initiator's CW was disabled prior to hanging up on the held party, it remains disabled after the customer answers the ringback.
- Flashes are ignored after a two-way call has been set up to a 911 attendant. This means that for the duration of the 911 call, the TWC feature cannot be used.

- A customer involved in a two-way call can flash and use TWC to add-on a 911 attendant. All subsequent flashes will be ignored.

Call Waiting Interaction

The following interactions pertain to call waiting (CW):

- If a line has call forwarding on busy (CFB) and CW, the CW service normally takes precedence over CFB.
- Given a line that has both CFB and CW and is in a talk state, the first call attempting to terminate is treated as a CW call. Subsequent termination attempts will be call forwarded (that is, CFB is invoked only if a call is already waiting).
- If CW treatment cannot be given (for example, because the line is dialing or ringing), then CFB takes effect.
- CW and CCW cannot be invoked simultaneously.
- When CW is disabled via CCW, it only applies to calls terminating at the subscriber line. It does not affect calls terminating at other subscriber lines.
- During a call to a 911 attendant, the CW service is inhibited (that is, no CW tone).

Calling Number Delivery Interaction

The following interactions pertain to the calling number delivery (CND) feature:

- No CND data is sent during or after a CW tone.
- CND data is sent for held and waited parties during the first silent interval of ringback that results from the customer going on hook in response to a CW tone.

CHAPTER 6

Interactive Voice Response Functions

Revised: March 24, 2011, OL-12606-21

The Cisco BTS 10200 Softswitch supports interactive voice response (IVR) functions for the remote activation call forwarding (RACF) and screening list editing (SLE) features. To use the RACF feature, the user dials a specified directory number (DN—assigned by the service provider) and is connected to the appropriate IVR media server. The user enters a personal ID number (PIN) to access the IVR functions, and follows the voice prompts of the IVR server to activate, deactivate, or edit RACF options.

To use the SLE feature, the user dials one of several vertical service code (VSC) numbers (in the form *xx) and is connected to the appropriate IVR media server. The user follows the voice prompts to edit screening lists.

This section includes IVR information on the following features:

- RACF, page 6-2
- Screening-List-Editing Services, page 6-7
- Two-Level Automatic Recall Activation, page 6-22
- No Solicitation Announcement, page 6-24
- Privacy Screening, page 6-38
- Multi-Lingual Support Feature, page 6-45

Note The IVR announcements and prompts presented in this appendix are based on standard audio files provided with the BTS 10200. Service providers can alter such audio files to suit particular service offerings. Therefore, the announcements and prompts presented in this guide might not match exactly those provided with specific implementations.

Furthermore, service providers can create names for services that differ from the names of the services in this document.

This section describes IVR functionality for the following features:

- RACF, page 6-2
- Screening-List-Editing Services, page 6-7
- Two-Level Automatic Recall Activation, page 6-22
- No Solicitation Announcement, page 6-24
- Privacy Screening, page 6-38

- Multi-Lingual Support Feature, page 6-45

RACF

RACF permits users to control their call forwarding unconditional (CFU) functions when they are away from the phone. The service provider sets up this function for the user, and designates a DN the user should call to access interactive voice response (IVR) functions that control the RACF feature. Once the RACF function is set up, the user can take the following actions from a remote station:

- Activate CFU
- Deactivate CFU
- Change the target DN of CFU

The procedure is similar to making call-forwarding changes at a home or local business phone but requires the additional step of dialing the remote location:

- The user dials a remote-access DN and is prompted to enter the DN of the home or local business phone and then the RACF authorization code (a PIN). The PIN can be shared by a group, or it can be unique to the individual subscriber.
- Once the user's PIN has been validated, the user's current CFU activation status is checked.
  - If the CFU feature is currently inactive (calls are not being forwarded), the user is prompted to enter a DN to which calls should be forwarded.
  - If the CFU feature is currently active (calls are being forwarded), the user is given the option of deactivating CFU or changing the DN to which a call should be forwarded.
- A subscriber with a unique PIN can change the PIN using the VSC function. (A specific VSC, for example * 9 8, is assigned and provisioned by the service provider.) The PIN can be changed only from the base phone.

For more information about RACF, see Chapter 3, "Subscriber Features."

Using IVR Functions for RACF

For a detailed description of RACF, see the "Call Forwarding Features" section in Chapter 3, "Subscriber Features."

To use the IVR functions to access the RACF feature, complete the following steps:

Step 1 Dial the number supplied by your service provider for RACF service. (See Figure 6-1.)

The media server plays the following announcement and prompt:

"Welcome to your remote access to the Call Forwarding feature. Please enter your home telephone number including area code."

Step 2 Enter your home phone number.

The media server plays the following prompt:

"You entered <number>. If correct, press 1.

If this is not correct, press 2."

The media server plays the following voice prompt:

"Enter your PIN."

Step 3 Enter your PIN.

Note Initially, you enter the PIN supplied by the service provider. The next time you attempt to access the RACF feature from a remote location, the system prompts you to change the PIN. See the "RACF PIN Change" section on page 6-5.

The media server plays the following announcement and prompt:

"You entered: <*PIN*>.

If correct, press 1.

If this is not correct, press 2."

Step 4 Assuming that you entered your PIN correctly, press 1.

The media server plays the following prompt:

"Please enter the number where you wish to forward your calls.

Step 5 Enter the number to which you want calls forwarded.

The media server plays the following voice prompt:

"You entered: <*xxx-xxx-xxx*>

If correct, press 1.

If this is not correct, press 2."

Note If the media server replayed your call-forwarding number incorrectly, enter 2. In this case, the server returns to the voice prompt for entering a call-forwarding number.

Step 6 Assuming that you entered your call-forwarding number correctly, press 1.

The media server plays the following voice prompt:

"Your calls are currently being forwarded to <*xxx-xxx-xxxx*>.

To keep forwarding calls to this number, press 1.

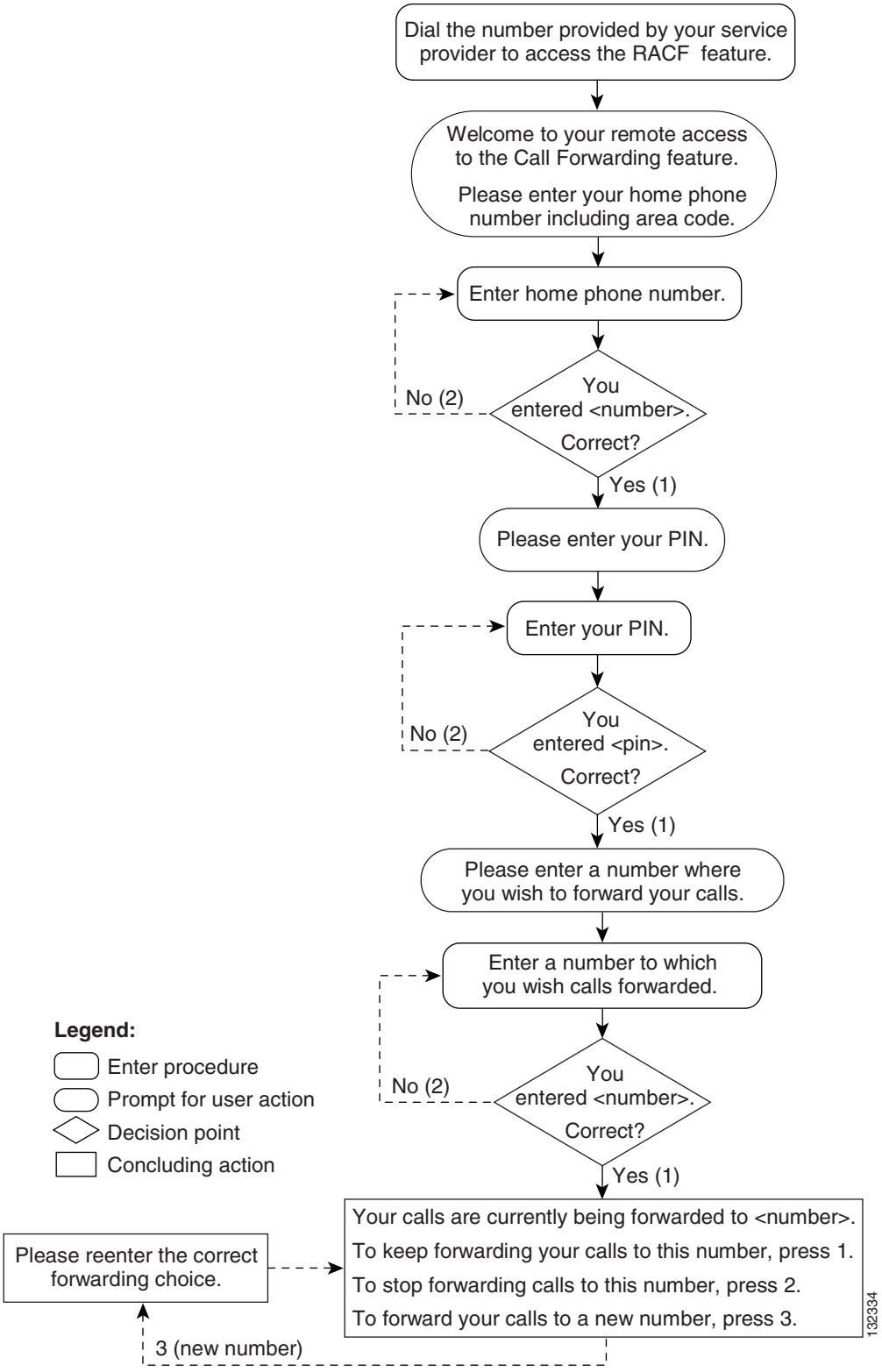
To stop forwarding calls to this number, press 2.

To forward your calls to a new number, press 3."

Step 7 Enter the number that corresponds to the option you want to use.

Figure 6-1 presents a flow chart that shows the sequence of IVR prompts and audio responses that pertain when you are using the RACF feature.

Figure 6-1 Remote Activation of Call Forwarding



RACF PIN Change

To use the RACF feature from a remote location (away from home phone) you must change the default PIN originally assigned by the service provider. If you do not change the PIN and then attempts to use the RACF feature, the media server plays an announcement stating that the PIN should be changed and access is denied.

You perform a PIN change from the home (or base) telephone.

Changing a PIN

To use the IVR announcements and prompts to change a previously established PIN (or the PIN initially supplied by the service provider), complete the following steps from the home (or base) telephone:

Step 1 To access the IVR system to change the PIN, dial the RACF PIN-change VSC (typically * 9 8). (See Figure 6-2.)

The media server plays the following prompt:

"Please enter your PIN."

Step 2 Enter your PIN.

The media server plays the following voice prompt:

"Please reenter your PIN."

Step 3 Reenter your PIN.

The media server plays the following voice prompt:

"You entered <*xxxx*>.

If this is correct, press 1.

Note If you enter the PIN initially supplied by the service provider, you cannot access the RACF feature from a remote location.

If this is not correct, press 2."

Step 4 To change your PIN, press 2.

The media server plays the following voice prompt:

"Please enter your new PIN number."

Step 5 Enter your new PIN.

The media server plays the following voice prompt:

"Please reenter your new PIN number."

Step 6 Reenter you new PIN number.

"You entered <*xxxx*>.

If this is correct, press 1.

If this is not correct, press 2."

Note The system supports a specified number of attempts to confirm the PIN change. If you try to exceed that number, the system denies further access and plays the announcement, "You do not have access to the PIN change feature. Goodbye."

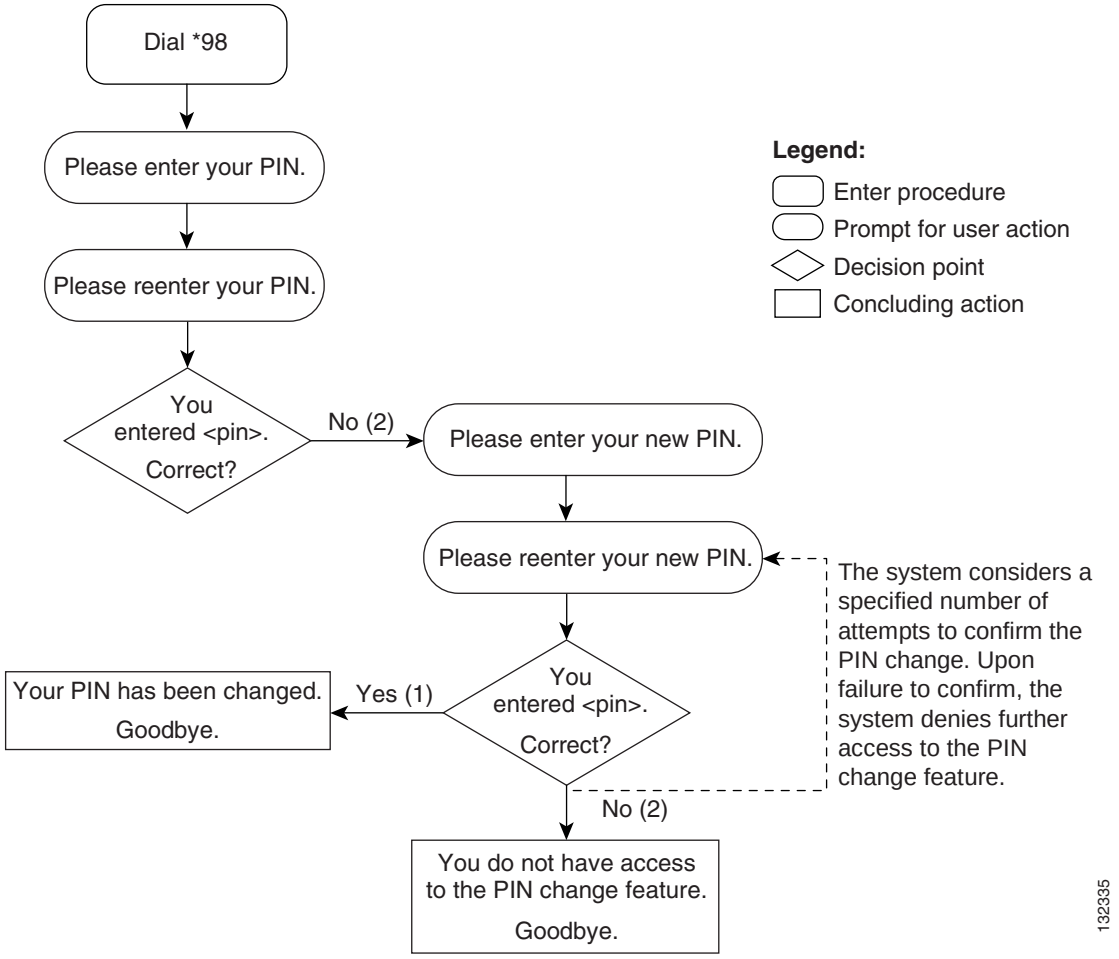
Step 7 Press 1.

The media server plays the following voice announcement:

"Your PIN has been changed. Goodbye."

Figure 6-2 presents a flow chart that shows the sequence of IVR prompts and audio responses when you are changing the PIN required to use the RACF feature.

Figure 6-2 Changing the RACF PIN



Screening-List-Editing Services

This section describes how to use IVR functions from a handset to operate a number of screening-list-editing services. These services include Selective Call Forwarding (SCF), Selective Call Acceptance (SCA), Selective Call Rejection (SCR), and Distinctive Ring/Call Waiting (DR/CW). For a detailed description of these services, see Chapter 3, "Subscriber Features."

Using IVR for Selective Call Forwarding

To use the Selective Call Forwarding service to specify a forward-to number and a list of DNs from which calls will be forwarded, complete the following steps:

Step 1 Initiate SCF service by dialing * 6 3 or * 8 3. (See Figure 6-3.)

The system plays the following voice announcement to indicate whether the service is currently on or off:

"Your Selective Call Forwarding service is now off.

There are no entries on your list.

You may interrupt announcements at any time by entering a command key. When you are finished, hang up.

Note If you interrupt the announcements, enter the command key immediately after its corresponding option is announced. For example, press the number-sign key (#) immediately after the announcement: "To add an entry, press the number-sign key."

The system then announces the set of key commands that you can enter to perform the various screening-list-editing operations offered by the SCF service.

To turn this service on, press 3.

To add an entry, press the number-sign key.

To remove one or more entries, press the star key.

To remove all list entries, press 0 8.

To remove all anonymous list entries, press 0 9.

To hear the entries on your list, press 1.

To hear these instructions repeated, press 0."

Step 2 Press 3.

The system plays the following voice prompt:

"To turn this service on, you must add an entry to your list.

Please enter the number to which you want your calls forwarded, followed by the number-sign key."

Step 3 Enter the number, and press #. (See Figure 6-4.)

The system plays the following voice announcement and prompt:

"Your calls will be forwarded to <*xxx-xxx-xxxx*>.

If this number is correct, press 1.

If this number is not correct, press 0."

If you enter 0, the system returns to the initial prompt for entering the forward-to number.

Step 4 Press 1.

Step 5 Press # to add a number to the list from which calls will be forwarded.

The system plays the following voice prompt:

"There are no entries on your list.

Enter the number to be added, then press the number-sign key.

To add the last-calling party, press 0 1, followed by the number-sign key."

Note If you attempt to enter a number that is already on your list, the system plays the announcement: "The number <*number*> is already on your list. Please continue. Press 0 for instructions or hang up."

Step 6 Enter the number and press #.

The system plays the following voice announcement and prompt:

"The number <*xxx-xxx-xxxx*> has been added to your list.

Please continue. Press 0 for instructions or hang up."

Step 7 To add the last-calling party, press 0 1 #. (See Figure 6-5.)

The system plays one of the following voice announcements:

"The number <*xxx-xxx-xxxx*> has been added to your list."

or:

"The number you have added is an anonymous entry."

The system then plays the following prompt:

"Please continue. Press 0 for instructions or hang up."

Step 8 Continue or hang up.

Note If you press 0, the system repeats the entire initial announcement of the available options. You can select an option immediately after it is announced.

Figure 6-3 presents a flow chart that shows the initial announcement and list of command options for implementing and managing the Selective Call Forwarding service.

Figure 6-3 Selective Call Forwarding—Initial Announcement and List of Commands

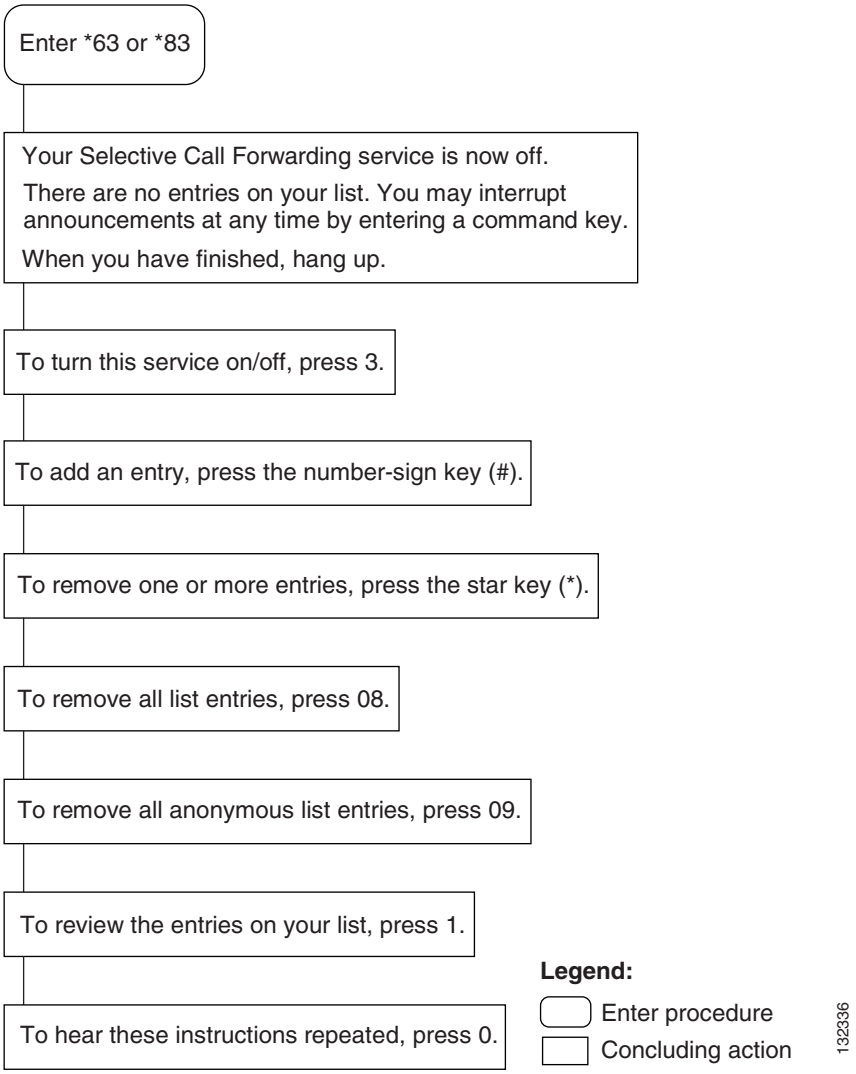


Figure 6-4 presents a flow chart that shows the sequence of IVR prompts and audio responses for activating the Selective Call Forwarding service and adding a forward-to number.

Figure 6-4 Selective Call Forwarding—Adding the Forward-to Number

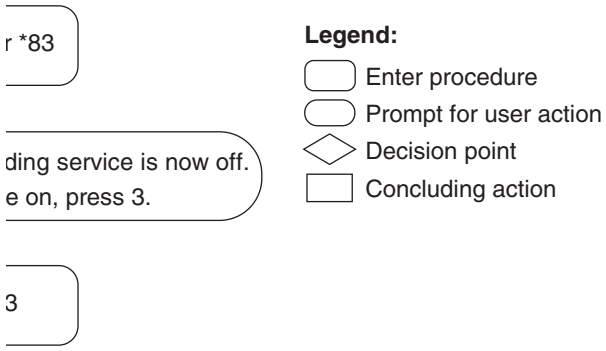
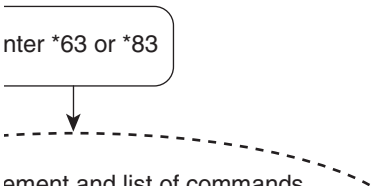


Figure 6-5 presents a flow chart that shows the sequence of IVR prompts and announcements for activating the Selective Call Forwarding service and adding DNs from which calls will be forwarded.

Note In the following figures, the elliptical element with a dashed border represents the announcement of the full set of command options. The element contained within ellipse represents the selected key command.

Figure 6-5 Selective Call Forwarding—Adding a Number or Last Calling Party



Selective Call Forwarding—Listing and Deleting Entries

To use the Selective Call Forwarding service to list and then delete one or more of the numbers from which calls will be forwarded, complete the following steps. (See Figure 6-6.)

Step 1 To hear a voice listing of the entries on your list, press 1.

The system plays the following voice announcement and prompt:

"There are <*number*> entries on your list.

To delete an entry,
press 0 7 as soon as you hear it.

You may enter a list-editing command at any time, including 0 for the list of commands.

The first entry on your list is <xxx-xxx-xxxx>.
Next <xxx-xxx-xxxx>.

This is the end of your list. Please continue. Press 0 for instructions or hang up."

Step 2 Press 0 7 as soon as you hear a number that you want to delete, or press the star key.

If you press *, the system plays the following prompt:

"Enter the number to be deleted then press the star key.

To delete the last-calling party, press 0 1 followed by the star key."

Step 3 Enter the number you want to delete and press *.

The system plays the following prompt:

"The number <xxx-xxx-xxxx> has been deleted from your list. Please continue. Press 0 for instructions or hang up."

or:

"The number to be removed is not on your list. Please continue. Press 0 for instructions or hang up."

Step 4 To delete all entries on your list simultaneously, press 0 8. (See Figure 6-7.)

The system plays the following announcement:

"There are no more entries on your list."

Step 5 To delete all anonymous entries on your list, press 0 9. (See Figure 6-8.)

The system plays the following announcement:

"There are no more anonymous entries on your list. Please continue. Press 0 for instructions or hang up."

or:

"We're sorry, there are no entries on your list. Please continue. Press 0 for instructions or hang up."

Step 6 To turn the SCF service off, press 3

The system plays the following announcement:

"Your Selective Call Forwarding service is now off."

Figure 6-6 presents a flow chart that shows the sequence of IVR prompts and announcements for using the Selective Call Forwarding service to review the list of DNs from which calls are forwarded and to delete DNs from the list.

Figure 6-6 Selective Call Forwarding—Listing and Deleting Entries

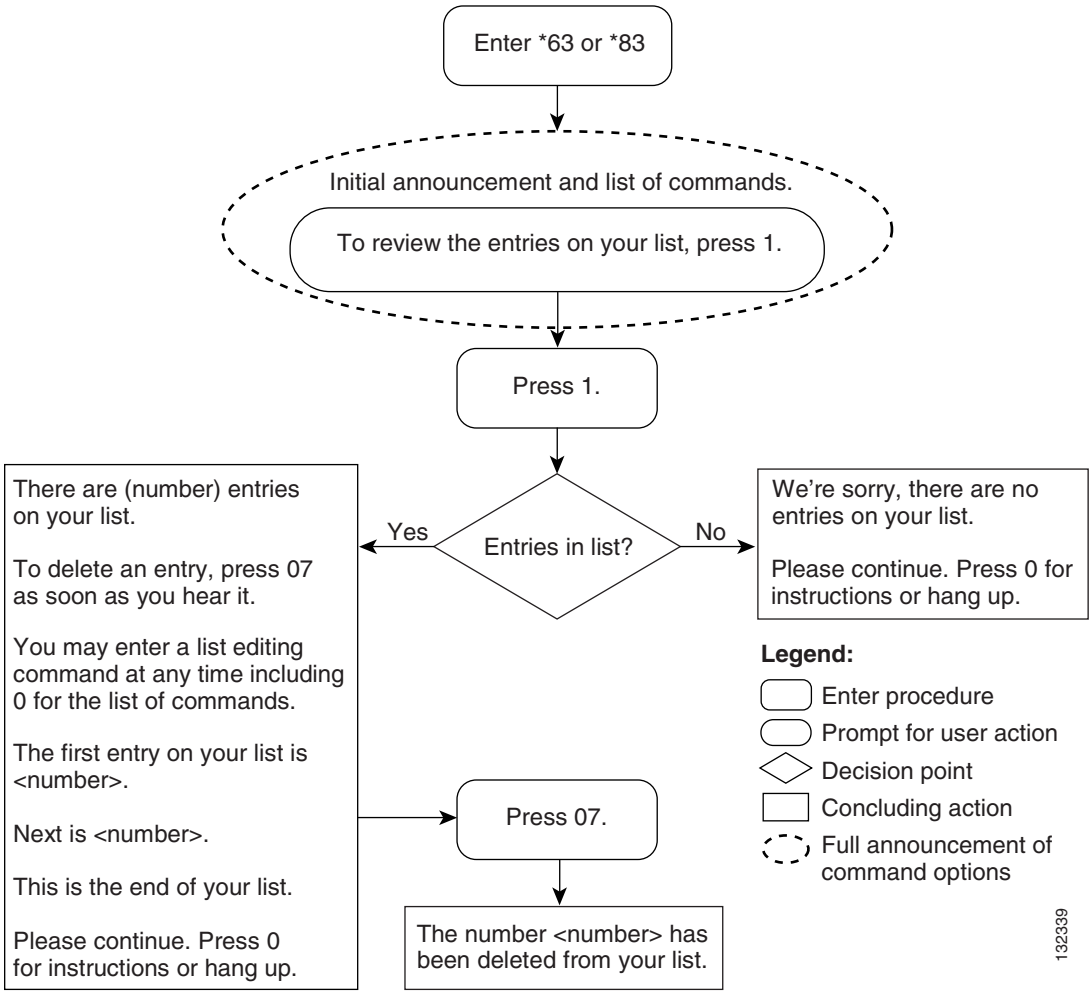


Figure 6-7 presents a flow chart that shows the sequence of IVR prompts and announcements for using the Selective Call Forwarding service to remove DNs from the list from which calls are forwarded.

Figure 6-7 Selective Call Forwarding—Removing All Entries from a List

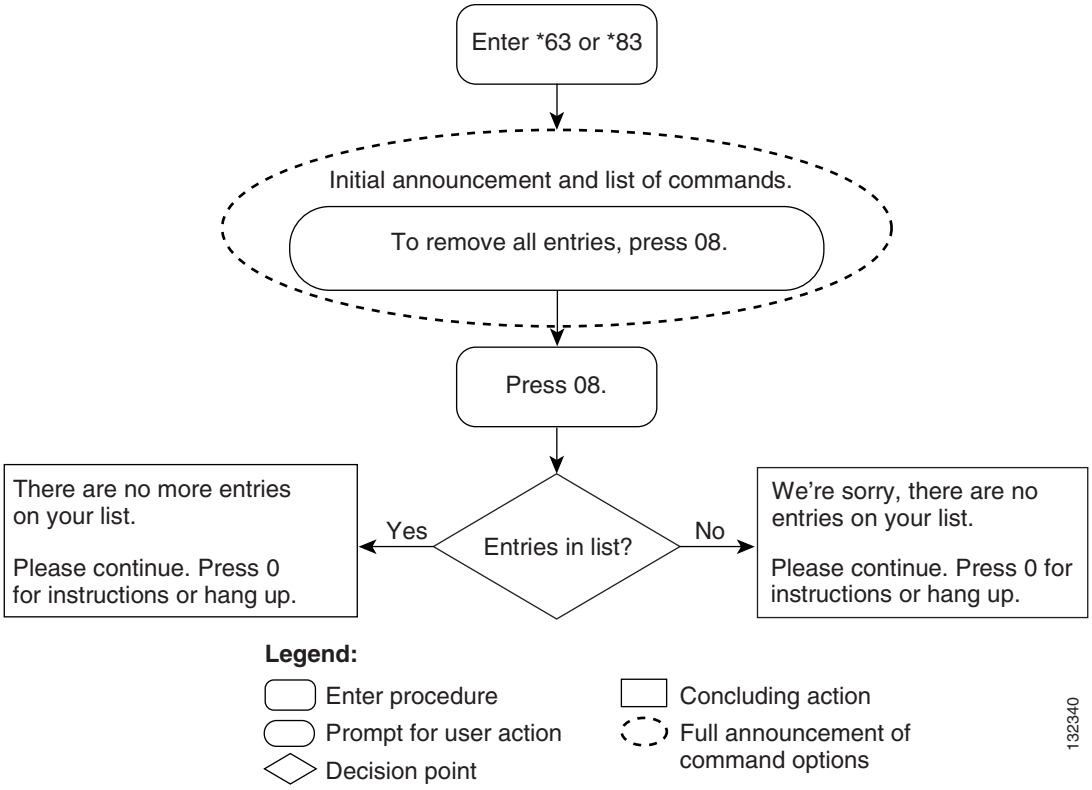
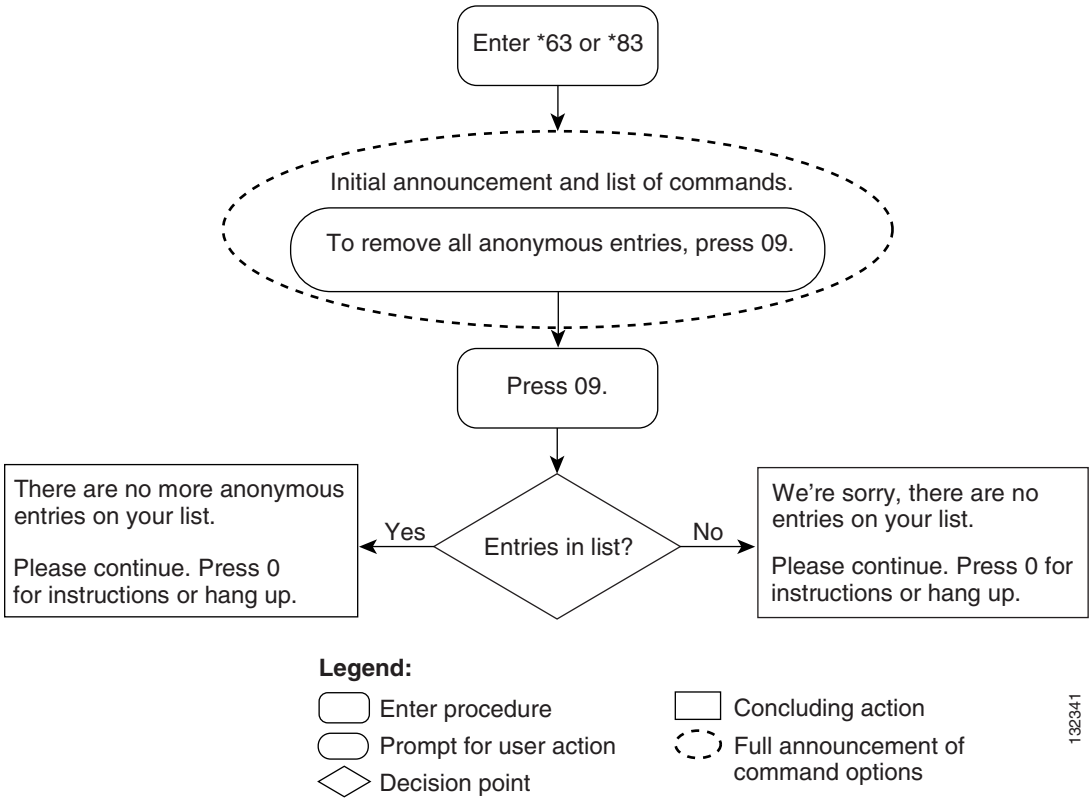


Figure 6-8 presents a flow chart that shows the sequence of IVR prompts and announcements for using the Selective Call Forwarding service to remove anonymous DNs from the list from which calls are forwarded.

Figure 6-8 Selective Call Forwarding—Removing All Anonymous Entries from a List



Using IVR for SCA, SCR, and DR/CW Services

The following sections provide generic descriptions of how a subscriber uses IVR functions to operate the Selective Call Acceptance, Selective Call Rejection, and Distinctive Ring/Call Waiting services. After you enter the specific VSC for the service you wish to access, the method for using the available options is identical, regardless of which service you select.

Note The figures in this section are also generic. The flow charts show that the command options for SCA SCR, and DR/CW operate identically.

For a detailed description of SCA, SCR, and DR/CW, see Chapter 3, "Subscriber Features."

Activating an IVR Service

To activate an IVR service and add a DN to the service list, complete the following steps:

Step 1 Initiate <service_name> by dialing * <VCS_code>.

The system plays the following voice announcement to indicate whether the service is currently on or off. It then announces the set of key commands that you can enter to perform the various screening-list-editing operations offered by the service.

"Your <*service_name*> service is now off.

There are no entries on your list.

You may interrupt announcements at any time by entering a command key. When you are finished, hang up.

Note If you interrupt the announcements, enter the command key immediately after its corresponding option is announced. For example, press the number-sign key immediately after the announcement: "To add an entry, press the number-sign key."

To turn this service on, press 3.

To add an entry, press the number-sign key.

To remove one or more entries, press the star key.

To remove all list entries, press 0 8.

To remove all anonymous list entries, press 0 9.

To review the entries on your list, press 1.

To hear these instructions repeated, press 0."

Step 2 Press 3.

The system plays the following voice prompt:

"There are no entries on your list. To turn this service on, you must add an entry to your list.

Enter the number to be added, then press the number-sign key (#)."

Note If the system detects that there is an entry already on your list, the system announces: "Your <*service_name*> service is now on. Please continue. Press 0 for instructions or hang up."

Step 3 Enter the number, and press #.

The system plays the following voice announcement and prompt:

"The number <*xxx-xxx-xxxx*> has been added to your list.

Please continue. Press 0 for instructions or hang up."

Step 4 To add the last-calling party, press 0 1 #.

The system plays one of the following voice announcements and prompt:

"The number <*xxx-xxx-xxxx*> has been added to your list."

or:

"The number you have added is an anonymous entry.

Please continue. Press 0 for instructions or hang up."

Step 5 Continue or hang up.

Note When you press 0, the system repeats the entire initial announcement of the available options. You can select an option immediately after it is announced.

Figure 6-9 presents a flow chart that shows the initial announcement and list of command options for implementing and managing an IVR service.

Figure 6-9 IVR Service—Initial Announcement and List of Commands

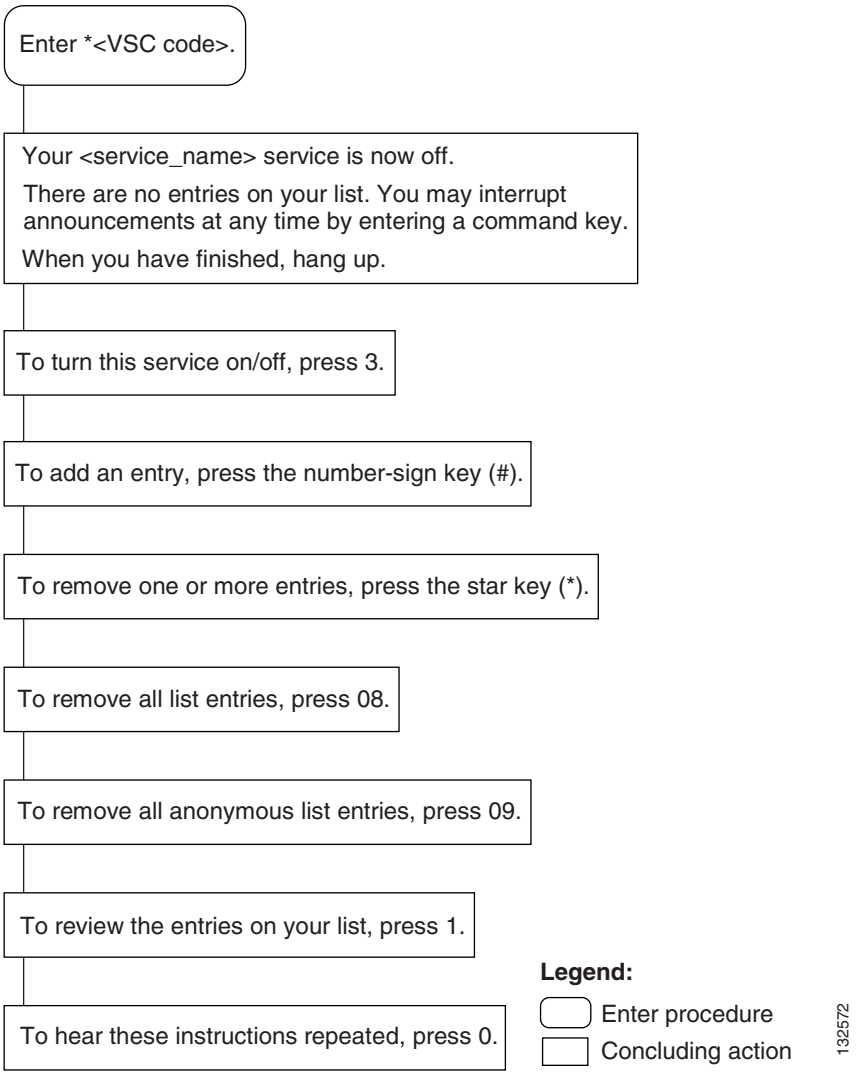


Figure 6-10 presents a flow chart that shows the sequence of IVR prompts and audio responses for activating the IVR service and adding DNs to the service list.

Figure 6-10 Adding a Number or Last Calling Party

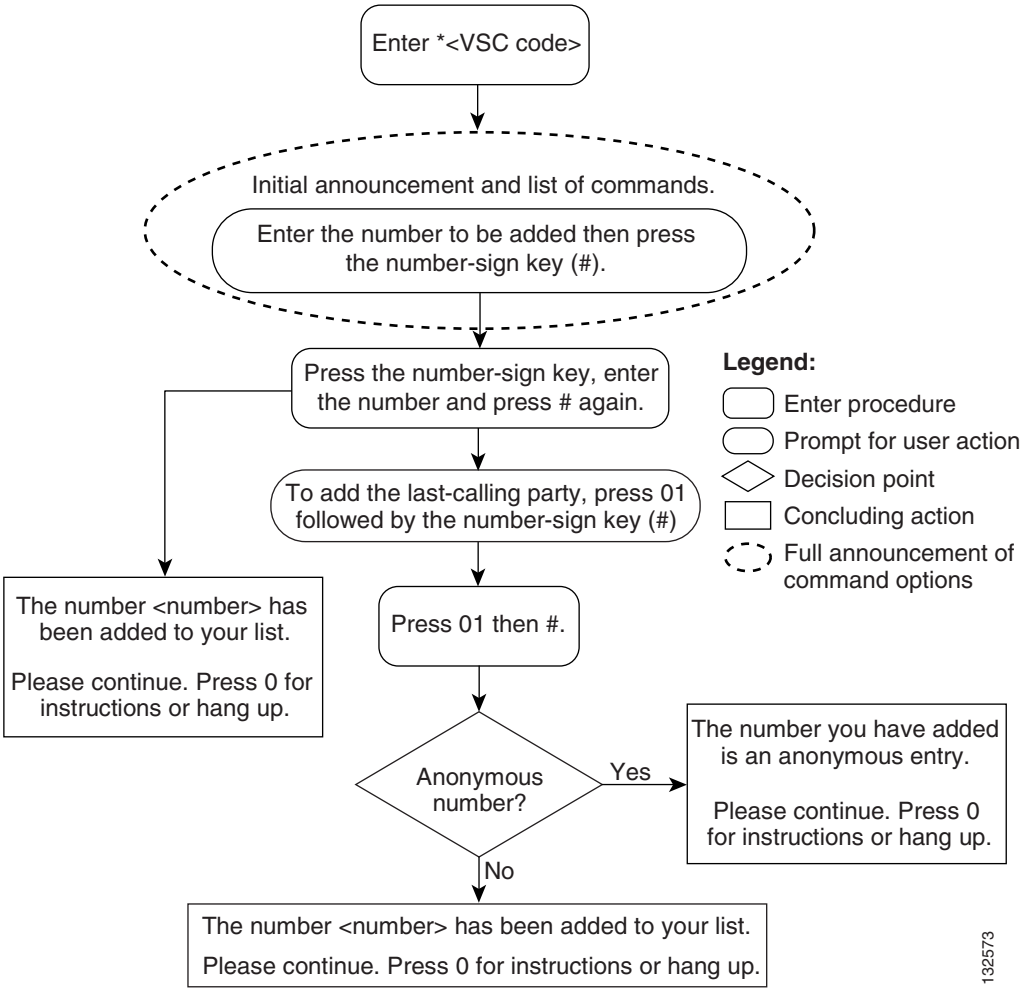
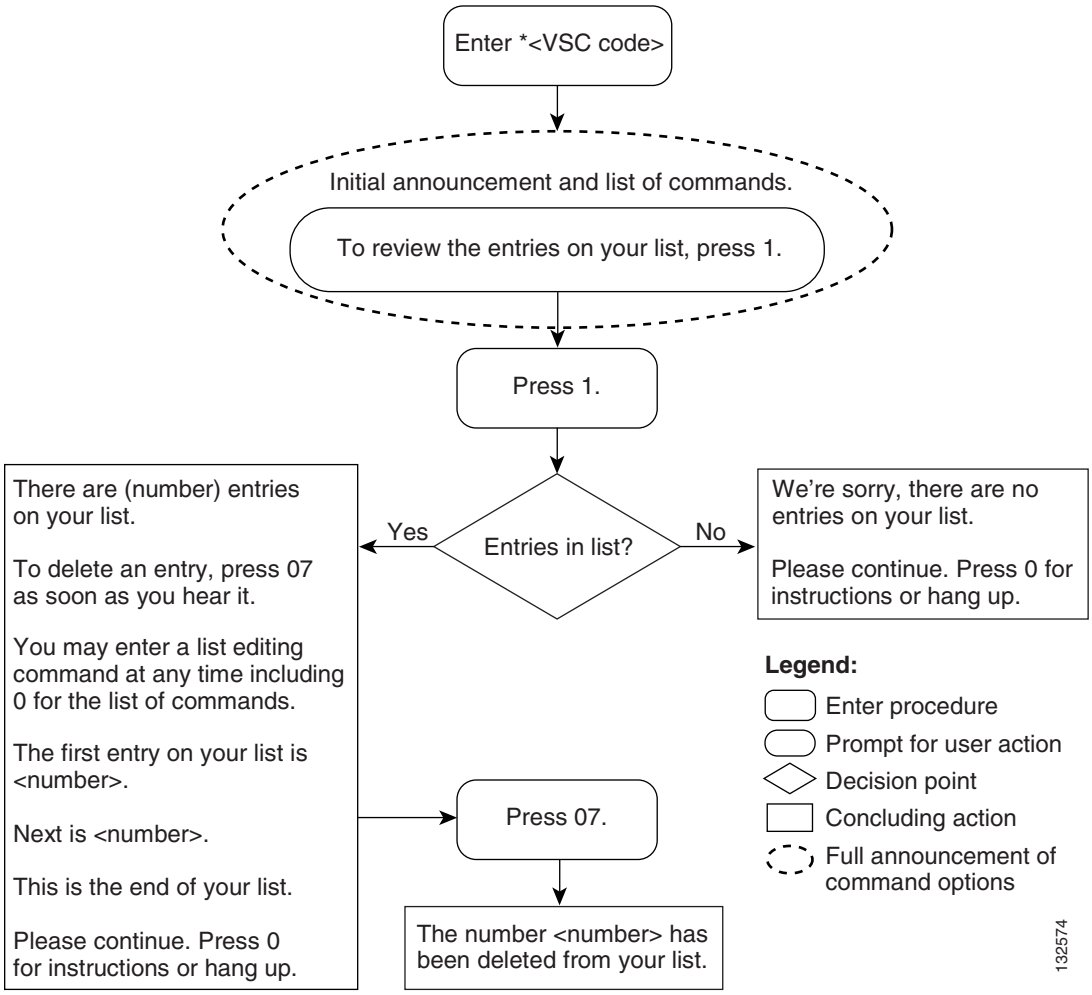


Figure 6-11 presents a flow chart that shows the sequence of IVR prompts and audio responses for reviewing the list of DNs for a service.

Figure 6-11 Selective Call Forwarding—Reviewing List Entries



Deleting Numbers from the Service List

To use an IVR service to list and then delete one or more of the numbers from the service list, complete the following steps:

Step 1 To hear a voice listing of the entries on your list, press 1.

The system plays the following voice announcement and prompt:

"There are <*number*> entries on your list.

To delete an entry,
press 0 7 as soon as you hear it.

You may enter a list-editing command at any time, including 0 for the list of commands.

The first entry on your list is <*xxx-xxx-xxxx*>.
Next <*xxx-xxx-xxxx*>.

This is the end of your list. Please continue. Press 0 for instructions or hang up."

Step 2 Press 07 as soon as you hear a number that you want to delete or press the star key.

If you press *, the system plays the following voice prompt:

"Enter the number to be deleted, then press the star key.

To delete the last-calling party, press 0 1 followed by the star key."

Step 3 Enter the number you want to delete and press *.

The system plays the following voice prompt:

"The number <*xxx-xxx-xxxx*> has been deleted from your list. Please continue. Press 0 for instructions or hang up."

or:

"The number to be removed is not on your list. Please continue. Press 0 for instructions or hang up."

Step 4 To delete all entries on your list simultaneously, press 0 8.

The system plays the following announcement:

"There are no more entries on your list."

Step 5 To delete all anonymous entries on your list, press 0 9.

The system plays the following announcement:

"There are no more anonymous entries on your list. Please continue. Press 0 for instructions or hang up."

or:

"We're sorry, there are no entries on your list. Please continue. Press 0 for instructions or hang up."

Step 6 To turn the SCA service off, press 3

The system plays the following announcement:

"Your <*Service_Name*> service is now off."

Figure 6-12 presents a flow chart that shows the sequence of IVR prompts and audio responses for removing all DNs from the service list.

Figure 6-12 Removing All Entries from a Service List

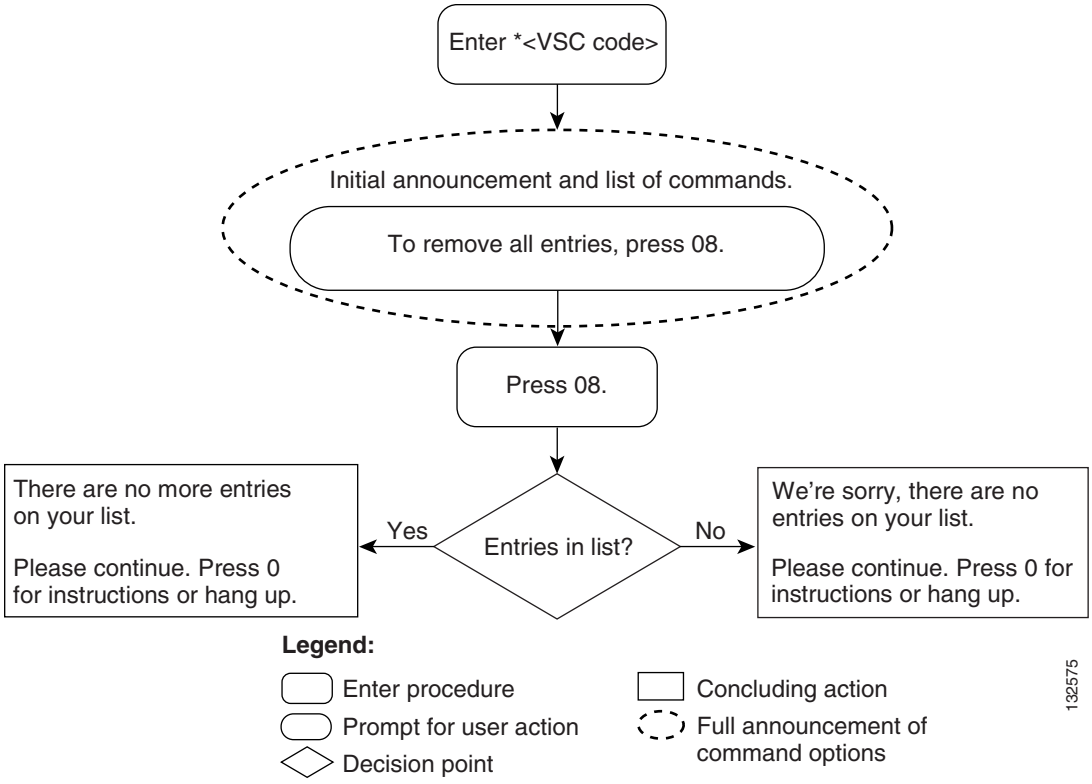
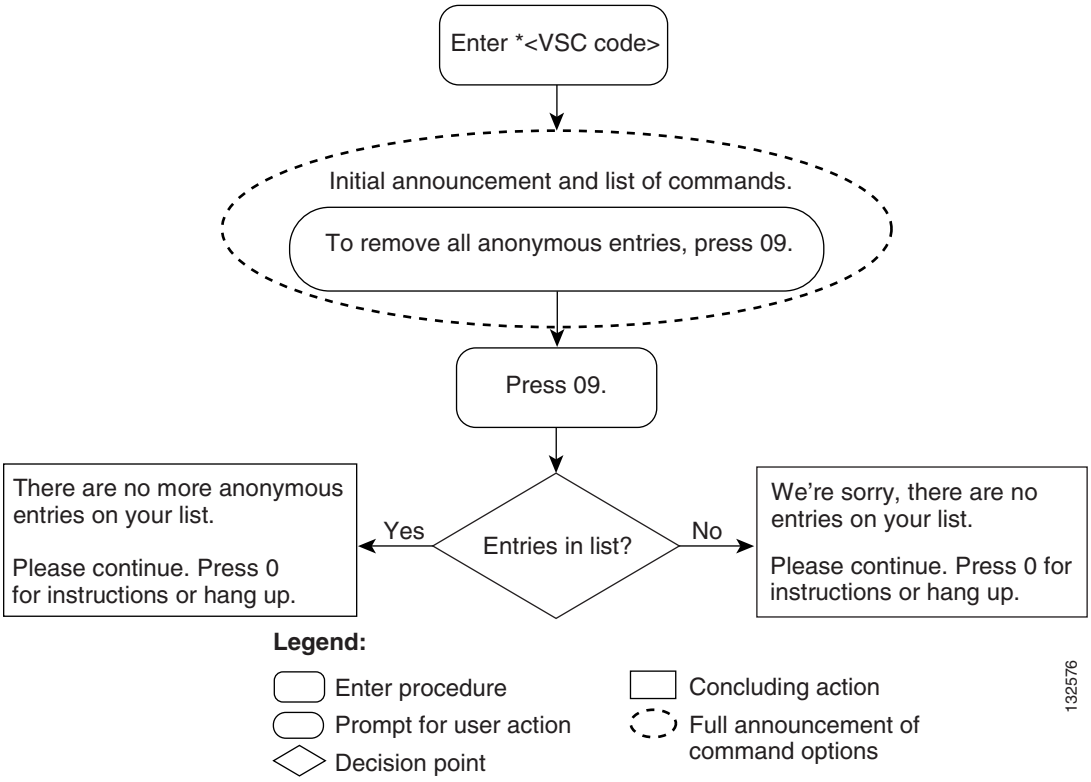


Figure 6-13 presents a flow chart that shows the sequence of IVR prompts and audio responses for removing all anonymous DNs from the service list.

Figure 6-13 Removing All Anonymous Entries from a Service List



Two-Level Automatic Recall Activation

Two-Level Automatic Recall (AR) activation is an extension of one-level AR, which requires communication with an IVR server. The IVR server generates the announcement of the calling-party number, provides appropriate voice prompts, and collects the user's response.

To use the IVR functions to access the two-level AR feature, complete the following steps:

Step 1 As the two-level AR subscriber, do not pick up (go off hook) in response to an incoming call until the phone stops ringing. (See Figure 6-14.)

Step 2 Lift the handset (go off hook).

Step 3 Dial * 6 9.

The system plays one of the following two announcements:

- "The last incoming number was <*number*>. This call was received on <*MM:DD:YYYY*> at <*HH:MM*>. To activate Automatic Recall, dial 1; otherwise, hang up."
- "The last incoming number was an anonymous number and cannot be announced. To activate Automatic Recall, dial 1; otherwise, hang up."

Note The subscriber has 7 seconds to dial 1.
(This is a provisional timer that can be set to a duration from 1 to 10 seconds.)

If the time elapses, the system announces:
"We're sorry, please hang up now. Consult your written instructions and try again later."

Step 4 Dial 1.

Whether the last incoming call was announced or anonymous, the system determines the status of the calling number and, depending on that status, performs one of the following actions.

Note By default, the Cisco BTS 10200 does not permit AR of an anonymous number. To enable AR of an anonymous number, in the ca-config table, you must provision the TYPE token to ARAC-ACTIVATION-TO-ANONYMOUS-DN and set the value to Y (Yes). Unless enabled, in response to an attempt to use AR for an anonymous caller, the system plays the following announcement:

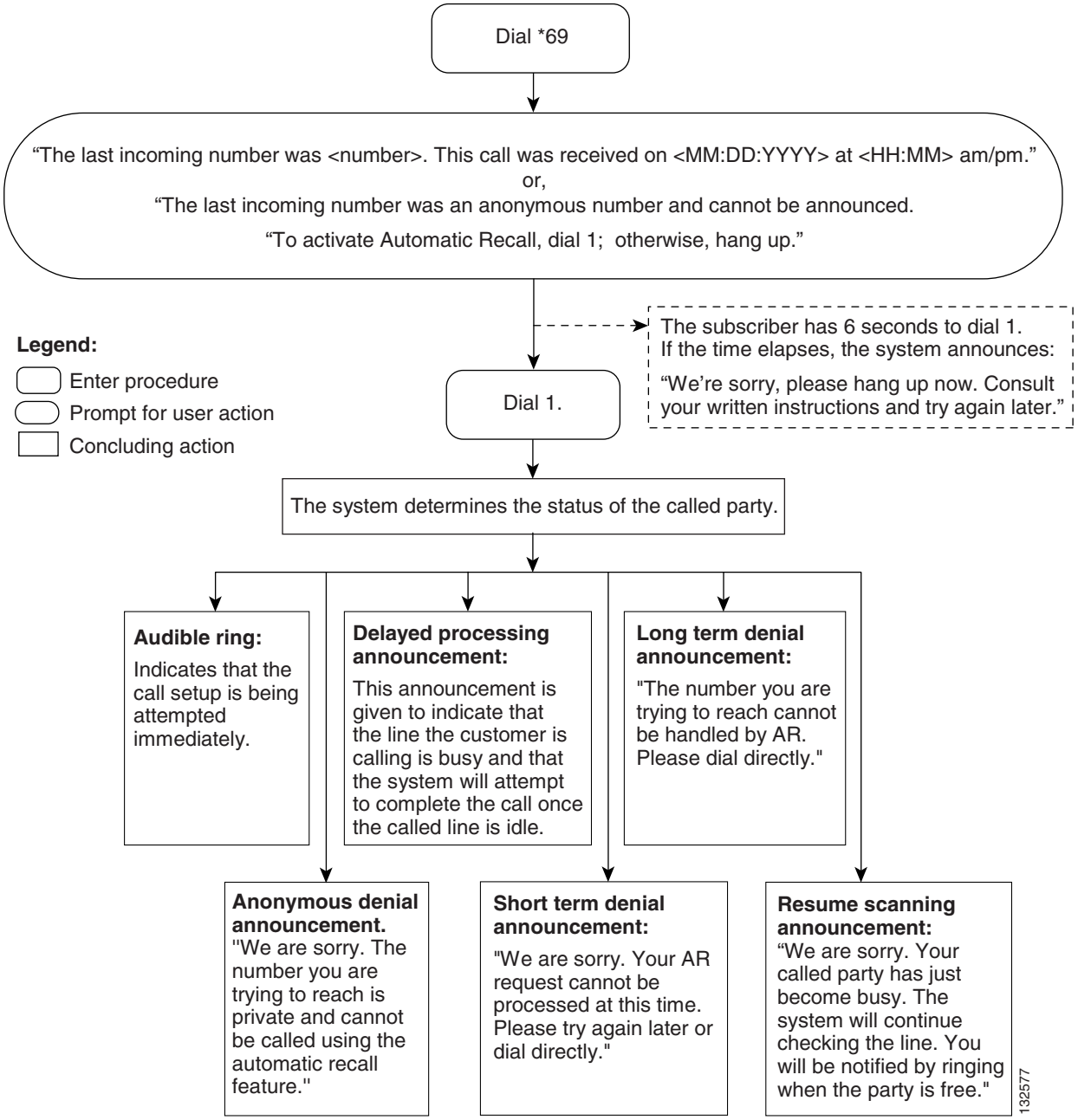
"We are sorry. The number you are trying to reach is private and cannot be called using the automatic recall feature."

- Audible ring—Indicates that the call setup is being attempted immediately.
- Delayed processing announcement—"The number you are calling is busy. The system will check the line for the next 30 minutes. You will be notified by ringing when the party is free."
- Short term denial announcement—"We are sorry. Your automatic recall request cannot be processed at this time. Please try again later or dial directly."
- Long term denial announcement—"The number you are trying to reach cannot be handled by automatic recall. Please dial directly."
- Resume scanning announcement—"We are sorry. Your called party has just become busy. The system will continue checking the line. You will be notified by ringing when the party is free."

Step 5 Respond appropriately to the specific announcement played by the system.

Figure 6-14 presents a flow chart that shows the sequence of IVR prompts and audio responses when you are using two-level activation of AR.

Figure 6-14 Two-Level Automatic Recall



No Solicitation Announcement

The No Solicitation Announcement (NSA) service enables a subscriber to announce to callers, whose phone numbers are not added to an NSA-bypass list, that the subscriber is not accepting calls. The subscriber can define the time interval during which the no-solicitation announcement is played to every caller whose DN is not on the bypass list.

A caller who receives the no-solicitation announcement can continue the call by pressing a key specified in the announcement (by default, the digit 1) or by waiting on the line.

The feature also enables the subscriber to:

- Activate or deactivate the feature
- Change a PIN, which (if authentication is enabled for the NSA service) is required before the subscriber can change NSA settings)
- Create the NSA bypass list
- Alter the schedule during which the NSA is active

Typically, a caller who attempts to contact the NSA subscriber during a time when the service is scheduled and active hears the following announcement:

> "You have reached a number that does not accept solicitations. If you are a solicitor, please add this number to your do-not-call list and hang up now. Otherwise, press 1 or stay on the line."

The subscriber can maintain a bypass list of complete or partial DNs. A call made from a listed DN is accepted. The system does not play the NSA announcement to callers from DNs on the NSA-bypass list.

The subscriber can also turn this feature on or off and can set a time schedule (start and end times) when this feature is active. The billing record indicates whether the solicitor hangs up when the announcement is played.

The feature has two subfeatures, Invocation and Activation:

- Invocation plays a message to callers who are not on the subscriber's no-solicitation bypass list during the time set by the subscriber. The message notifies the caller that the subscriber is not accepting solicitation calls, but the caller can press 1 if the caller wishes to complete the call. If the caller presses 1, the subscriber's phone rings.
- Activation enables the subscriber to manage the no-solicitation bypass list of complete or partial DNs from which calls are accepted. With this subfeature, the subscriber can:
  - Change the PIN (pass code) once (which is required for access to this menu)
  - Establish the schedule when the service is active
  - Turn off the service completely for all incoming calls

This sub-feature is called Activation.

Note For detailed procedures for provisioning and managing the NSA feature on the Cisco BTS 10200, see the feature module document entitled *No Solicitation Announcement Feature*.

NSA Activation

The NSA activation feature enables a subscriber to manage the following no-solicitation preferences:

- The time schedule when the NSA service is active
- The no-solicitation bypass list of DNs for callers enabled to bypass the no-solicitation announcement
- The PIN (once only)

A caller whose DN is not on the subscriber's no-solicitation bypass list and whose call does not go through to the subscriber can do one of the following:

- The caller can stay on the line or press 1. In response to either of these decisions, the subscriber's phone rings and the caller is connected to the subscriber.
- The caller can hang up. In this case, the subscriber's phone does not ring.
- The caller can press a digit other than 1. In this case, the no-solicitation announcement is replayed to the caller. When a CLI-provisioned threshold of attempts is reached, the subscriber's phone rings and the caller is connected to the subscriber.

Note To activate the NSA service, the subscriber must enter at least one DN on the NSA bypass list.

Creating the NSA Bypass List

The NSA bypass list of DNs can include the following:

- Full DNs—If the full DN of the calling party matches the DN provisioned in this table, the system treats this as a match and allows the incoming call to bypass the NSA announcement.

  For example, if the subscriber adds the full DN 214-555-1234 to the NSA bypass list, the caller's number must match that number exactly. If the subscriber enters a number for a seven-digit area, the number is normalized.
- Extensions—For Centrex groups only, if the full extension of the calling party matches the DN provisioned in this table, the system treats this as a match and allows the incoming call to bypass the NSA announcement.

  For example, if the Centrex group adds the extension 501 to the NSA bypass list, a callers extension must match 501 to bypass the no-solicitation announcement.

Note If the subscriber line is not provisioned as a Centrex line, the system will not allow this option.

- Partial DNs—The system uses the longest possible match. If the calling number is 2145556789, the system matches as follows:
  - If the bypass list contains 214 (partial DN), 214555 (partial DN), and 2145556789 (full DN), the full DN is matched first.
  - If the bypass list contains 214 (partial DN) and 214555 (partial DN), but no full DN, the partial string 214555 is matched first.

The NSA bypass list can include up to 25 entries.

Establishing an NSA Schedule

The NSA service enables the service provider or a subscriber to set the time period when the NSA service will be active.Typically, a subscriber sets a start time, stop time, start day, and stop day. For example, a subscriber could make these entries: start time 8:00 a.m. (entered as 0800), stop time 5:00 p.m. (entered as 1700), start day Monday (entered as 1), and stop day Friday (entered as 5). Such settings would make the NSA service active from 8:00 a.m. Monday until 5:00 p.m. Friday.

When the NSA service is inactive, the subscriber's no-solicitation bypass list is preserved. During times when the NSA service is not scheduled, it is considered inactive.

Because it is possible that the Cisco BTS 10200 and a subscriber might not be located in the same time zone, the NSA schedule uses the time zone information present in the point of presence (POP) to which the subscriber belongs. If a time slot is not assigned to a subscriber for a feature, by default, the feature is considered always active. In provisioning the Cisco BTS 10200 feature table, the service provider can control whether a subscriber can set NSA schedules by interactive voice response (IVR) handset provisioning.

Note If the Subscriber Time of Day Schedule (subscriber-tod-schedule) table is not provisioned for a subscriber, the system checks the POP table for that subscriber, and looks up the value of a VIRTUAL-NSA-SUBSCRIBER-ID token. If a subscriber-tod-schedule is provisioned for this virtual subscriber, the system uses that schedule. Otherwise, the system treats NSA as always active for that subscriber. See the feature module document entitled *No Solicitation Announcement Feature*.

PIN Management

If the service provider enables authentication for the NSA service, the subscriber must enter a PIN to authenticate access to that service. When access is successfully authenticated, the subscriber can change the settings of the NSA service. The PIN can be a number from 1 to 26 digits.

The service provider can disable a PIN check for the NSA service by provisioning the feature-config table. This would enable a subscriber to manage the NSA service without passing PIN authentication.

Note The service provider can enable (or disable) the PIN authentication step by setting the AUTH-ENABLED token to Y (or N) in the Feature Configuration (feature-config) table. The default value is Y.

The service provider provisions a value for PIN in the service-feature-data table. After that, the service provider enables a subscriber to alter the PIN one time. To enable a subscriber to alter the PIN one time. To enable the subscriber to alter the PIN, the service provider provisions the PIN and sets the PINTYPE to NEWPIN. If PINTYPE is not set to NEWPIN, the service provider retains maintenance of the PIN and, therefore, control of the authentication to access and manage the NSA service options.

If the PINTYPE is not NEWPIN and the PIN is not present, the authentication for access to the NSA service fails.

Caution Authentication to access the NSA service should be controlled by a PIN entry. Otherwise, anyone who has access to a subscriber's handset, and knows the VSC code for the NSA service can gain unauthorized access to management of the subscriber's NSA service.

Managing the NSA Service

A NSA service subscriber can perform the following operations using a handset:

- Authenticate access to manage the service
- Change feature status (active/inactive)
- Add or delete a specific entry
- Delete all entries
- Delete all anonymous entries

- Review and delete an entry during review
- Repeat the menu instructions
- Manage the active timeslot

NSA—Initial Authentication and PIN Change

When accessing the NSA service for the first time, the subscriber enters the password (PIN) provided by the service provider and then (if the service provider has set PINTYPE TO NEWPIN), the subscriber is prompted to change the password to one the subscriber chooses. The subscriber can set the PIN only once. Thereafter, the subscriber must contact the service provider to change the PIN.

To authenticate access to the NSA service, complete the following steps:

Step 1 Enter * 9 4.

The system plays the following voice prompt:

"Please enter your password now."

Step 2 Enter the password provided by the service provider.

If you enter the password incorrectly, the system plays the following announcement:

"We are sorry, the password you entered is incorrect. Please hang up and try your call later."

If you enter the password correctly, the system plays the following prompt:

"You must now change your password. Please enter a new password now."

Step 3 Enter your new password.

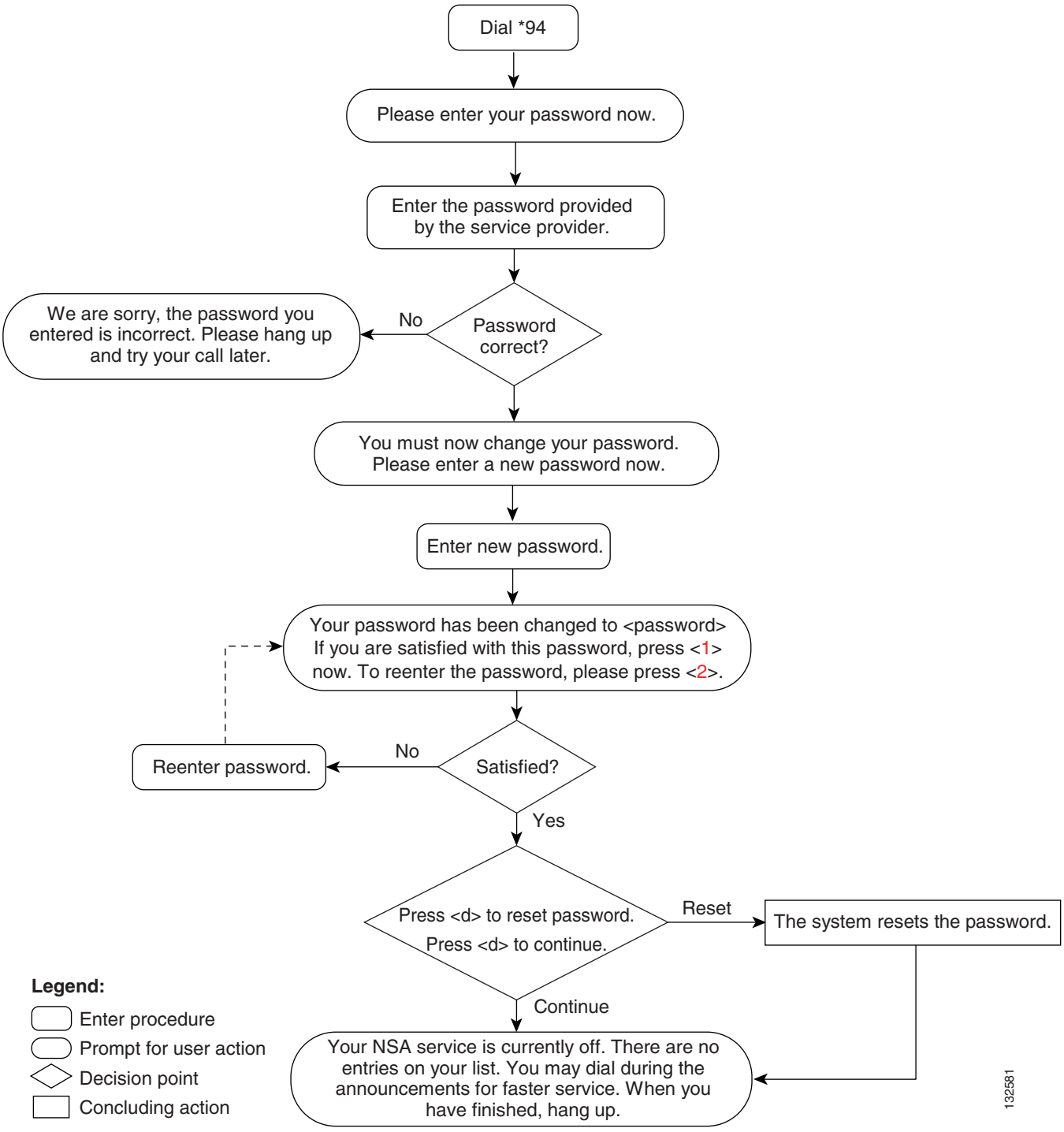
The system plays the following announcement:

"Your password has been changed to <*xxx...*>. If you are satisfied with this password, press 1."

Step 4 If you are satisfied with your password, press 1.

Figure 6-15 presents a flow chart that shows the IVR prompts and announcements that are played when PINTYPE is set to NEWPIN and the subscriber is enabled to change the PIN (one time only).

Figure 6-15 No Solicitation Announcement—PIN Change



Managing NSA Service Options

After the subscriber either passes the PIN check or accesses the NSA service directly (with authentication disabled), the subscriber can control activation of the service and manage service options.

To access and manage the NSA service, complete the following steps:

Step 1 Enter * 9 4

The system responds in one of two ways:

- If authentication is disabled for the NSA service in the feature-config table, the system plays the NSA service menu.
- If authentication is enabled for the NSA service in the feature-config table, the system plays the PIN authentication prompt.

When the subscriber accesses the NSA service, the system plays the following voice announcement to indicate whether the service is currently on or off. It then announces the set of key commands that one can enter to perform the various operations offered by the service.

> "Your NSA service is currently off.
>
> There are no entries on your list.
>
> You may interrupt announcements at any time by entering a command key. When you have finished, hang up.

Tip If you want to interrupt the announcements, enter the command key immediately after its corresponding option is announced. For example, press the number-sign key (#) immediately after the announcement: "To add an entry, press the number-sign key."

> To turn this service on, press 3.
>
> To add an entry, press the number-sign key.
>
> To remove one or more entries, press the star key.
>
> To remove all list entries, press 0 8.
>
> To remove all anonymous list entries, press 0 9.
>
> To hear the entries on your list, press 1.
>
> To schedule based on the time-of-day schedule, press 2.
>
> To hear these instructions repeated, press 0.
>
> Please dial now."

Step 2 Press the key that corresponds to the operation you wish to perform.

NSA—Adding DNs to the NSA List

A caller whose DN is on the NSA bypass list does not receive the NSA announcement.

Initially, you must add a number to the NSA bypass list in order to turn the NSA service on. That is, if you want the service to play the NSA announcement to all callers not on your NSA bypass list (during the time when the service is scheduled to be active), you must have at least one DN on your list.

You can enter as many as 25 DNs on the NSA bypass list.

To add the DNs of callers whose calls you want to bypass the NSA announcement, complete the following steps:

Step 1 Enter * 9 4.

The system plays the following announcement:

"Your No Solicitation Announcement service is currently off. There are no entries on your list.

You may dial during the announcements for faster service. When you are finished, hang up.

To turn this service on, press 3.

To add an entry, press the number-sign key.

To remove one or more entries, press the star key.

To remove all list entries, press 0 8.

To remove all anonymous list entries, press 0 9.

To review the entries on your list, press 1.

To hear these instructions repeated, press 0.

To schedule this service, press 2."

Step 2 Press 3.

The system plays the following announcement:

"To turn on this service, you must add an entry to your list. To add an entry, please press the number-sign key. If you wish to hear this announcement repeated, please dial 0."

Step 3 Press the number-sign key to add a number to your NSA bypass list.

The system plays the following prompt:

"Dial the number to be added, then press the number-sign key again.

To add the last-calling party, press 0 1, then press the number-sign key again.

To add an extension, press 0 2, dial the number to be added, then press the number-sign key again.

Note If the subscriber line is not provisioned as a Centrex line, the system does not allow this option.

To add a wildcard (a partial DN), press 0 3, dial the number to be added, then press the number-sign key again. Please dial now."

Step 4 Enter the number and press the number-sign key.

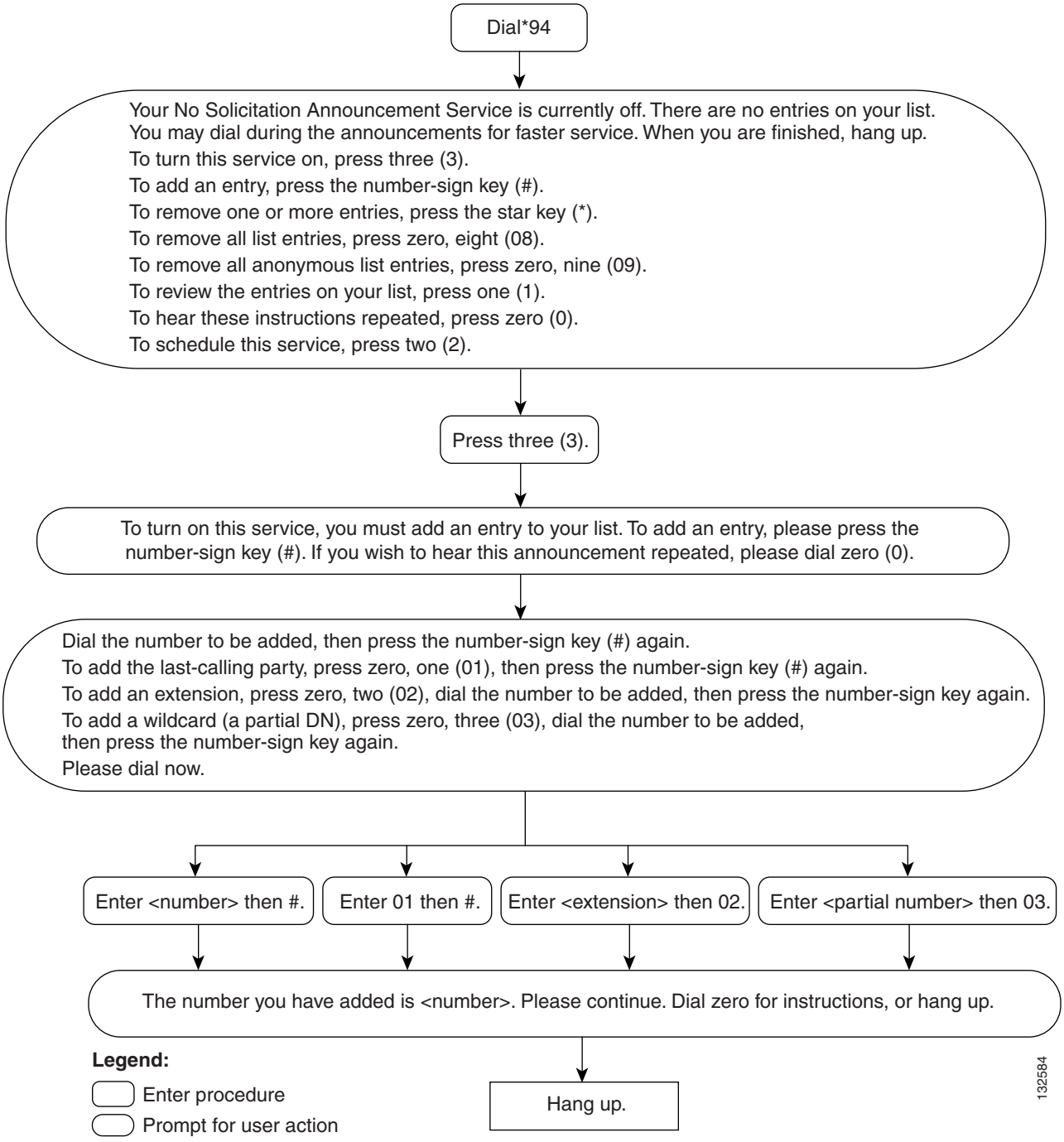
When you add a number to the NSA bypass list, the system plays the following announcement:

"The number you have added is <*number*>. Please continue. Dial 0 for instructions, or hang up."

Step 5 When you are finished adding numbers to the NSA bypass list, hang up.

Figure 6-16 presents a flow chart that shows the IVR prompts and announcements that are played when you are adding DNs to an NSA bypass list.

Figure 6-16 No Solicitation Announcement—Adding DNs to the NSA Bypass List



No Solicitation Announcement—Deleting DNs

To use the No Solicitation Announcement service to delete the DNs of callers who are allowed to bypass the NSA announcement, complete the following steps:

Step 1 Dial * 9 4 to access the NSA service.

Presuming that you previously entered DNs on your NSA bypass list and that you turned the service on, the system announces the set of key commands that you can enter to perform the various screening-list-editing operations offered by the NSA service.

"Your No Solicitation Announcement service is now on.

You may dial during the announcements for faster service. When you are finished, hang up.

To turn this service off, press 3.

To add an entry, press the number-sign key.

To remove one or more entries, press the star key.

To remove all list entries, press 0 8.

To remove all anonymous list entries, press 0 9.

To review the entries on your list, press 1.

To hear these instructions repeated, press 0.

To schedule this service, press 2."

Step 2 Press 1.

The system plays the following announcement and prompt:

"There are <*number*> entries on your list.

To delete an entry, press 0 7 as soon as you hear it.

You may enter a list-editing command at any time, including 0 for the list of commands.

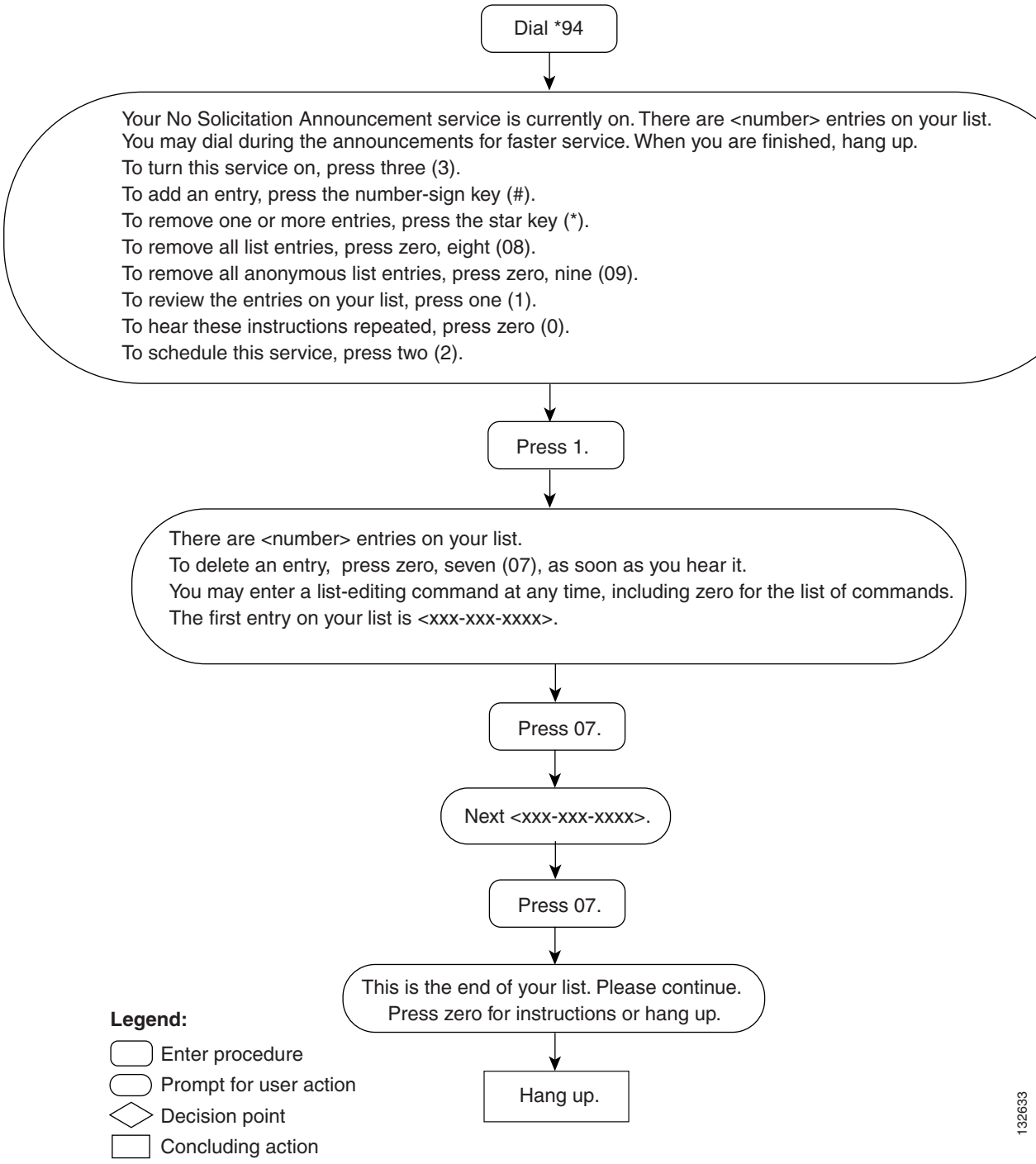
The first entry on your list is <*xxx-xxx-xxxx*>.
Next <*xxx-xxx-xxxx*>.

This is the end of your list. Please continue. Press 0 for instructions or hang up."

Step 3 Hang up.

Figure 6-17 presents a flow chart that shows the sequence of prompts and announcements that are played when you are deleting DNs from an NSA bypass list.

Figure 6-17 No Solicitation Announcement—Deleting DNs from the NSA List.



NSA—Scheduling the Service Time Slot

To schedule the time of day and days of the week during which the No Solicitation Announcement service applies, when activated, complete the following steps:

Step 1 Initiate NSA service by dialing * 9 4.

Presuming that you previously entered DNs on your NSA bypass list and that you turned the service on, the system announces the set of key commands that you can enter to perform the various screening-list-editing operations offered by the NSA service:

"Your No Solicitation Announcement service is now on.

You may interrupt announcements at any time by entering a command key. When you are finished, hang up.

To turn this service off, press 3.

To add an entry, press the number-sign key.

To remove one or more entries, press the star key.

To remove all list entries, press 0 8.

To remove all anonymous list entries, 0 9.

To review the entries on your list, press 1.

To hear these instructions repeated, press 0.

To schedule this service, press 2."

Step 2 Press 2 to schedule the NSA service.

If a schedule for the NSA service was previously set, the system plays the following prompt:

"Your NSA service is scheduled to be on from <*time_of_day*><*day_of_week*> to <*time_of_day*><*day_of_week*>. If you are satisfied with this schedule, please press one now. To set a different time-of-day schedule, press 2. Please dial now."

If no schedule was previously set, the system plays the initial prompt for setting the start time:

"Please enter the start time in 24-hour format."

Step 3 Enter the start time in 24-hour format (for example, 0700 for 7:00 a.m.).

If you enter the start time incorrectly, the system plays the following prompt:

"That was an invalid time. The time value should be between 0 and 2359. The end time must be later than the start time."

If you enter the start time correctly, the system plays the following prompt:

"Please enter the start weekday. 0 stands for Sunday, 6 stands for Saturday."

Step 4 Enter the value for the start weekday. (For example, 1 for Monday.)

If you enter the weekday incorrectly, the system plays the following announcement:

"That was an invalid day. The day value should be from 0 to 6."

If you entered the start weekday correctly, the system plays the following prompt:

"Please enter the end time in 24-hour format." (The end time must be later than the start time.)

Step 5 Enter the end time in 24-hour format.

If you enter the end time correctly, the system plays the following prompt:

"Please enter the end weekday. 0 stands for Sunday, 6 stands for Saturday."

Step 6 Enter the value for end weekday. (For example, 1 for Monday.)

If you enter the weekday incorrectly, the system plays the following announcement:

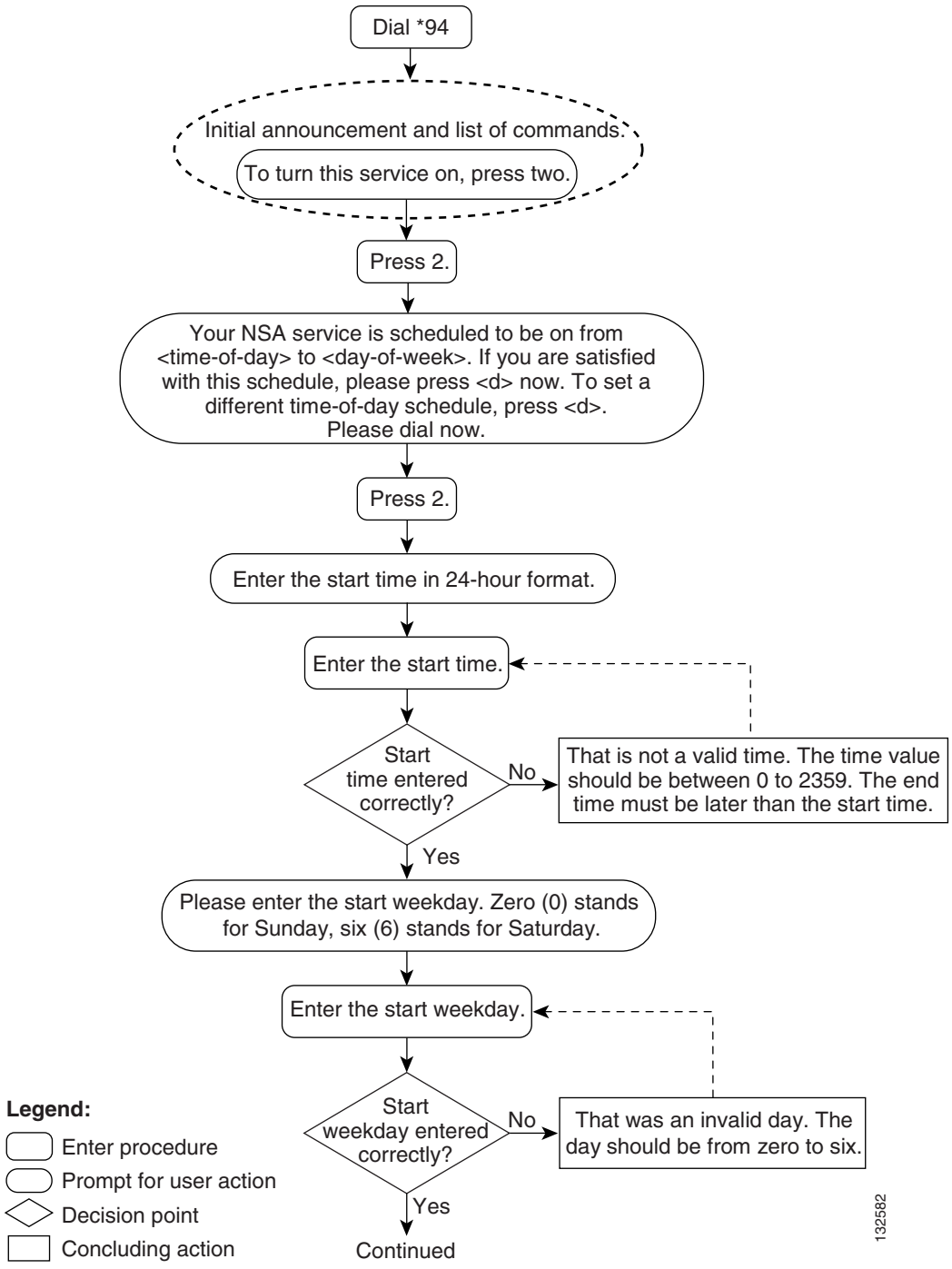
"That was an invalid day. The day should be from 0 to 6."

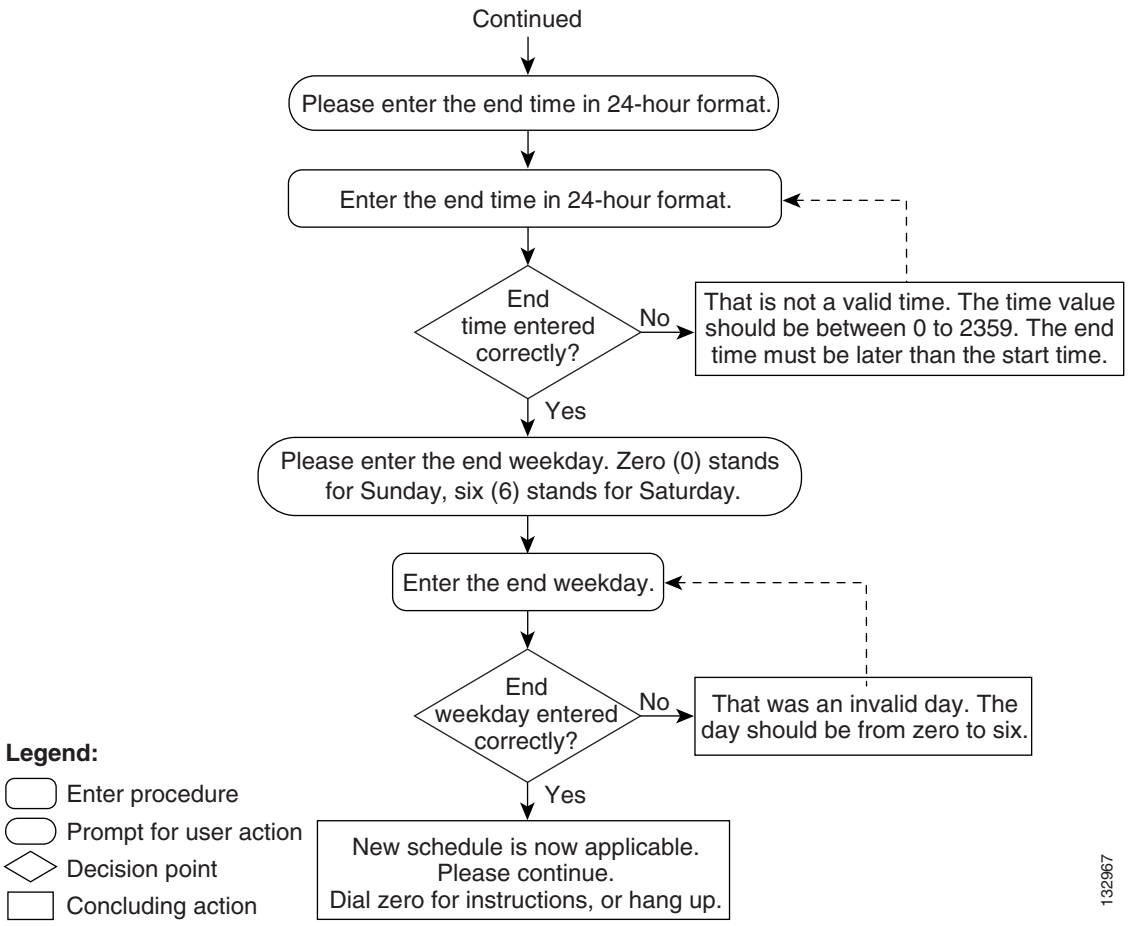
If you enter the end weekday correctly, the system plays the following prompt:

"New schedule is now applicable. Please continue. Dial 0 for instructions, or hang up."

Figure 6-18 presents a flow chart that shows the IVR prompts and announcements that are played when you are scheduling the service time interval for the No Solicitation Announcement service.

Figure 6-18 No Solicitation Announcement—Scheduling





Privacy Screening

The Privacy Screening feature enables a subscriber to accept or reject an anonymous call based on a short message (usually the caller's name) recorded by the caller. When a caller encounters the Privacy Screening message, the feature enables the caller to:

- Record a short message—After listening to the message, the subscriber can accept or reject the incoming call or forward it to voice mail.
- Enter a passcode (PIN)—Entering the correct passcode enables the caller to ring the subscriber and the call becomes a regular call.

This feature operates in conjunction with application and media servers, which comprise the IVR system.

For a detailed description of the Privacy Screening feature, see the "Privacy Screening (Calling Identity with Enhanced Screening)" section on page 3-111.

Subscriber Activation and Management of Privacy Screening

This section describes how a subscriber interacts with the IVR system to activate or deactivate Privacy Screening and to manage PIN authentication.

Step 1 The subscriber presses * 9 5.

The system plays the following announcement:

"Your Privacy Screening service is now <ON/OFF>. You may interrupt announcements at any time by entering a command key. When you have finished, hang up.

To turn the Privacy Screening feature <OFF/ON>, press 3.

To manage your PIN, press 4.

To hear these instructions repeated, press 0."

Pressing 3 toggles the feature ON or OFF.

Pressing 0 repeats the instructions.

Step 2 Press 4 to manage the PIN.

The system plays the following announcement:

"You have selected the PIN management option.

Please press 1 to set a PIN or press 2 to review and modify your PIN."

If the subscriber presses 1, the system plays the following announcement:

"Please enter a 4-digit PIN followed by the number sign."

If the subscriber presses 2, the system plays the following announcement:

"Your Privacy Screening service PIN is now set to <PIN>. If you wish to change this PIN, please enter your PIN followed by the number sign.

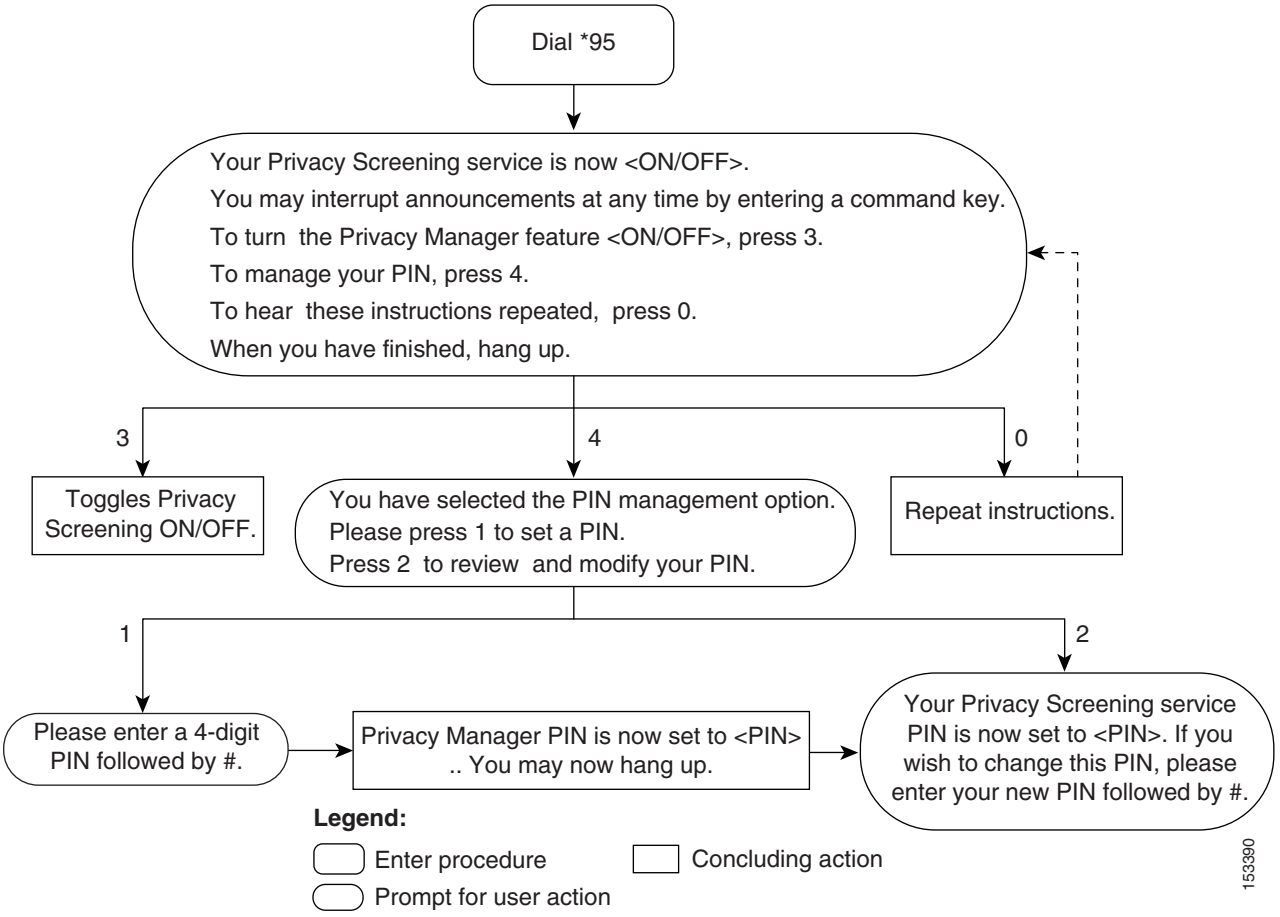
Step 3 The subscriber enters 1 or 2 and establishes the desired PIN.

The system plays the following announcement:

"Privacy Screening PIN is now set to <PIN>. You may now hang up."

Figure 6-19 presents a flow chart that shows the IVR announcements and prompts that are played when a Privacy Screening subscriber accesses the service to activate, deactivate or manage PIN authentication.

Figure 6-19 Privacy Screening Activation and PIN Change



Caller Interaction with Privacy Screening

This section describes how an anonymous caller interacts with the IVR system when attempting to place a call to a subscriber who has Privacy Screening activated. The caller is given the option of recording his name or entering a PIN.

Caller Name Recording

Step 1 The anonymous caller dials the Privacy Screening subscriber.

The system plays the following announcement:

> "The number you are calling does not accept anonymous calls. Please record your name at the tone and then press the number sign key; or, enter the 4-digit PIN."

Step 2 In this case, the caller speaks his name.

If the system records the name successfully, the call is placed to the subscriber.

If the system exceeds the maximum number of attempts allowed to record a name successfully, it plays the following announcement:

"Your recording is not clear. Please dial again later."

Caller PIN Entry

Step 1 The anonymous caller dials the Privacy Screening subscriber.

The system plays the following announcement:

"The number you are calling does not accept anonymous calls. Please record your name at the tone and then press the number sign key or enter the 4-digit PIN."

Step 2 In this case, the caller enters a PIN.

If the PIN is correct, the call is placed to the subscriber.

If the PIN is incorrect, the system plays the following announcement:

"Your PIN is incorrect. Please try again."

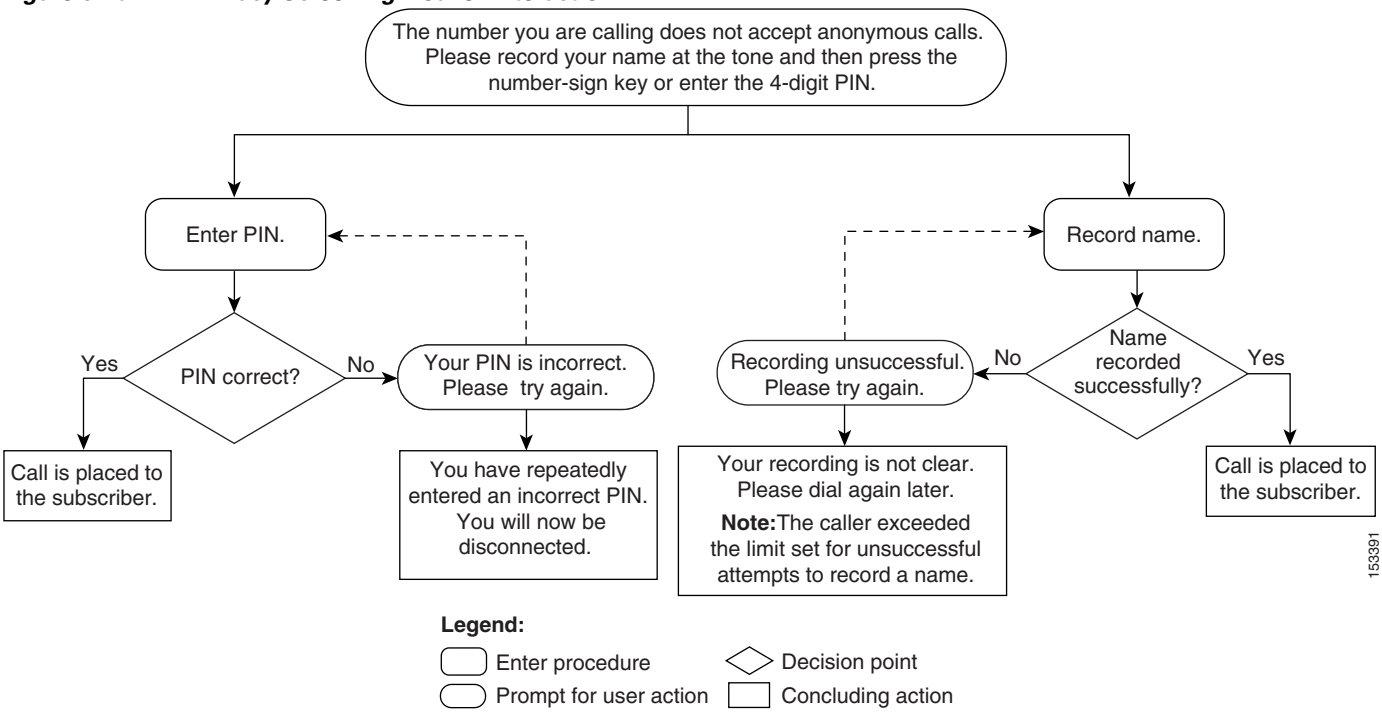
The system permits a configurable number of attempts to enter the correct PIN. When the caller exceeds the permitted number of attempts to enter the PIN, the system plays the following announcement:

You have repeatedly entered an incorrect PIN. You will now be disconnected.

Note If the application server is not reachable, incoming anonymous calls for the subscriber will be terminated on the subscriber.

Figure 6-20 presents a flow chart that shows the IVR prompts and announcements that are played when a caller attempts to call a subscriber who has Privacy Screening activated.

Figure 6-20 Privacy Screening—Caller Interaction



Subscriber Interaction with Privacy Screening

This section describes how a subscriber who has Privacy Screening activated interacts with the IVR system when an anonymous caller attempts a call.

Step 1 With Privacy Screening activated, the subscriber receives the call with a distinctive tone. When the subscriber picks up the call, the system plays the following announcement:

"This message is from your Privacy Screening service. You have an incoming call.

Press 1 to review the caller's name.

Press 2 to accept the call.

Press 3 to forward the call to voice mail if your are subscribed to voice mail.

Press 4 to play a 'not-available' announcement.

Press 5 to play a 'no-solicitation' announcement."

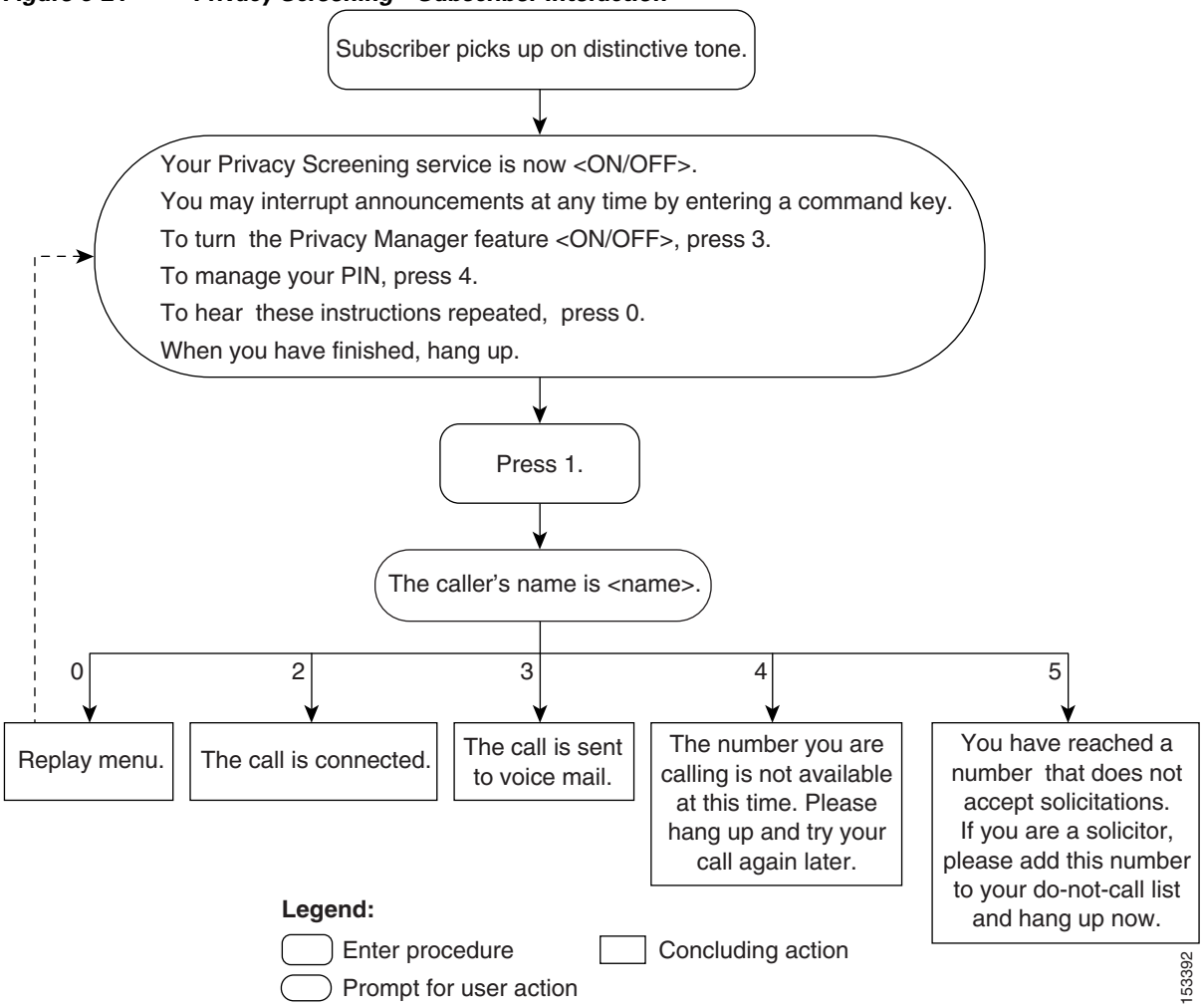
Press 0 to replay this menu at any time.

Step 2 The subscriber can enter one of the desired options or hang up to disconnect the call.

Note If the subscriber does not enter an option or if the subscriber presses a number not associated with one of the announced options, the system replays the option menu.

Figure 6-21 presents a flow chart that shows the IVR prompts and announcements that are played when a subscriber picks up the phone upon hearing the Privacy Screening distinctive tone.

Figure 6-21 Privacy Screening—Subscriber Interaction



Privacy Screening Announcements

Table 6-1 lists the Privacy Screening prompts played by the AS.

Table 6-1 Privacy Screening Announcements

Announcement Name	Announcement
PSmain_Bye_Ann	Thank you. Good bye.
PSmain-CdP_CgpHangsUp	The calling party has hung up.
PSmain_CdP_RejectCallNotify	The calling party will be notified that you have not accepted the call.
PSmain_CdPOptions_Ann	Press 1 to accept the call, press 2 to reject the call, or press 3 to redirect to voice mail.

Table 6-1 Privacy Screening Announcements (continued)

Announcement Name	Announcement
PSmain_CdPWelcome_Ann	Hi. You have a call from a number that cannot be identified. The caller name is
PSmain_CgPOption_EnterPinVoice	Welcome to Privacy Screening. Please enter your pin or record your voice at the tone. After recording, press pound.
PSmain_CgPOption_IncorrectEntry	Your entry cannot be accepted. Please try again.
PSmain_CgPOption_IncorrectEntryLast	You have repeatedly entered an incorrect entry. You will now be disconnected.
PSmain_CgPOption_IncorrectPin	Your pin is incorrect. Please try again.
PSmain_CgPOption_IncorrectPinLast	You have repeatedly entered an incorrect pin. You will now be disconnected.
PSmain_Failure_CallCompletionFailure	There is a technical problem, so your call cannot be completed.
PSmain_Failure_TransferCallFailed	Failed to transfer call.
PSmain_Hold_CallBeingConnectedAnn	Please wait while your call is being connected.
PSmain_Hold_CdpHangsUp	The called party has hung up.
PSmain_Hold_CdpRejectCall	The called party has rejected your call.
PSmain_Hold_Music	music
PSmain_Hold_NoAnswerAnn	There is no answer from the called party.
PSmain_Hold_TooManyTries	The called party has failed to accept your call.
PSmain_Record_IncorrectRecording	Recording unsuccessful. Please try again.
PSmain_Record_IncorrectRecordingLast	Your recording is not clear. Please dial again later.
PSmain_Record_Tone	tone

Privacy Screening Manage Announcements

Table 6-2 lists the Privacy Screening management announcements played by the AS.

Table 6-2 Privacy Screening Manage Announcements

Announcement Name	Announcement
PSpin_NewPassword_Enter	Please enter your new password.
PSpin_NewPassword_IncorrectFormat	Entered password format is incorrect. Please try again.
PSpin_NewPassword_NotChanged	Your password has not changed.
PSpin_OldPassword_Enter	Please enter your old password.
PSpin_OldPassword_Incorrect	Your old password is incorrect.
PSpin_Password_ConfirmChange	Please confirm password change by pressing 1, or press 2 not to change password.
PSpin_Password_Enter	Please enter your password.
PSpin_Password_Incorrect	Sorry, your password is incorrect.

Table 6-2 Privacy Screening Manage Announcements (continued)

Announcement Name	Announcement
PSpin_PhoneNo_Enter	Welcome to Privacy Screening Password and Management. Please enter your phone number and press pound.
PSpin_PhoneNo_Invalid	Invalid telephone number.
PSpin_Pin_Activity	Press 1 to add pin or press 2 to delete pin.
PSpin_Pin_Add	Please enter pin to add.
PSpin_Pin_Added	Pin has been added.
PSpin_Pin_Bye	Thank you goodbye.
PSpin_Pin_ConfirmAdd	Confirm and add by pressing 8, or press 9 not to add pin.
PSpin_Pin_ConfirmDelete	Please confirm and delete by pressing 8 or press 9 not to delete pin.
PSpin_Pin_Delete	Please enter the pin to delete.
PSpin_Pin_Deleted	Pin has been deleted.
PSpin_Pin_Exist	Entered pin already exists.
PSpin_Pin_IncorrectFormat	Entered format is incorrect.
PSpin_Pin_LimitExceeded	Your limit of adding pin has exceeded.
PSpin_Pin_NoPins	There is no more pins to delete.
PSpin_Pin_NotAdded	Pin has not added
PSpin_Pin_NotDeleted	Pin has not deleted
PSpin_Pin_Wrong	The entered pin does not exist
PSpin_Pin_WrongFailure	You have repeatedly entered an incorrect pin. You will now be disconnected
PSpin_SamePassword_Ann	Your new and old password is the same. Please try again
PSpin_SelectOption_Ann	Press 1 to change password, press 2 to change pin, or press * to cancel

Multi-Lingual Support Feature

This feature adds Multi-Lingual Support (MLS) for Interactive Voice Response (IVR) and announcement services. Using a Vertical Service Code (VSC), subscribers pick which language (English, French, or Spanish) to hear.

To provide IVR and announcement services, MLS works with the following Media Servers (MSs):

- IPUnity—IVR and announcements
- ThinkEngine Networks—IVR and announcements
- IOS Gateway—Announcements

An MS has four audio files for one IVR audio segment/announcement. For example each welcome.wav has three versions:

- eng_welcome.wav
- fra_welcome.wav

- spa_welcome.wav

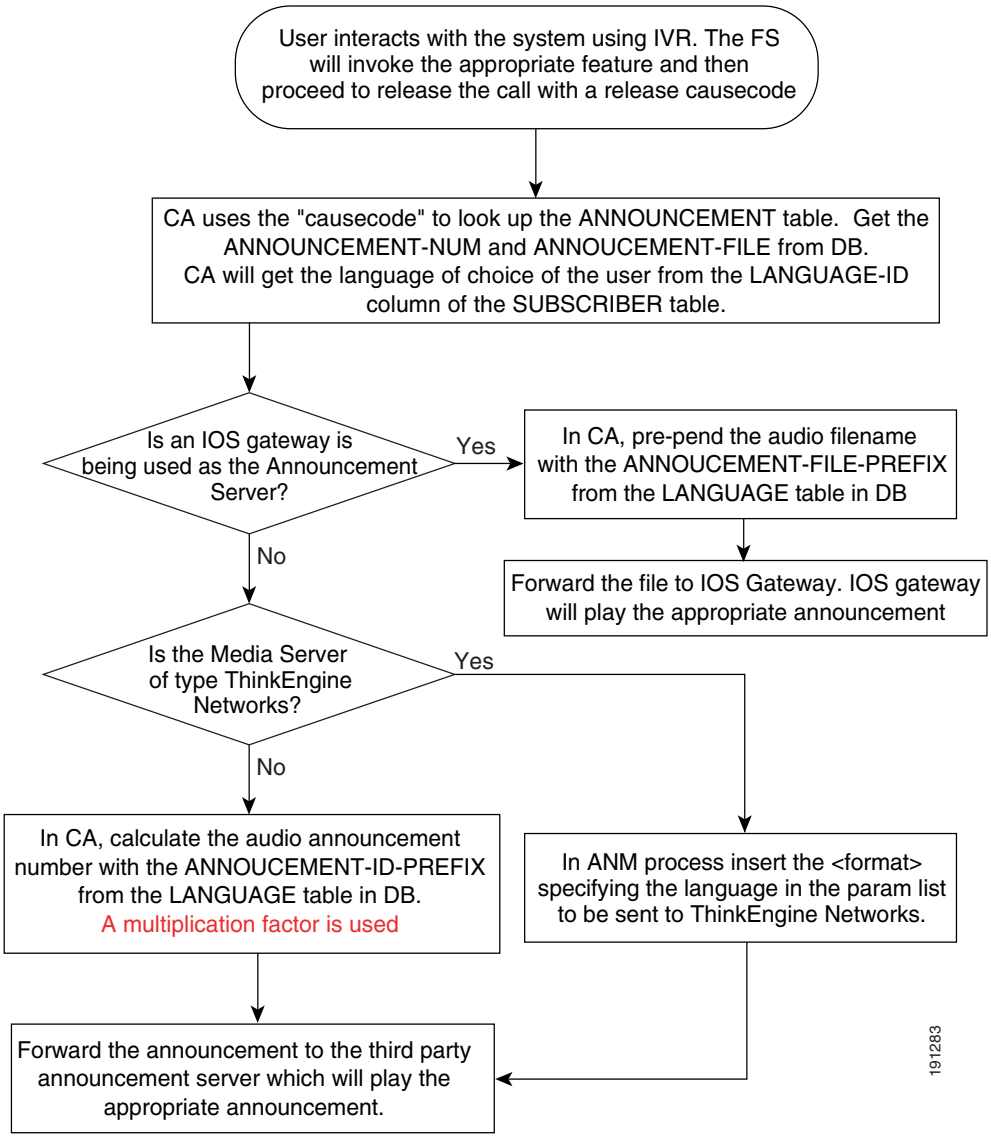
Using Basic Audio Utility Package (BAU) encoding MLS provides IVR service via a remote MS. If a provisioned language is different from the default, the BTS specifies BAU in the encoding field. BTS adds the language picked by the subscriber in variable audio segments:

```
?lang-<language of choice>
```

Using a Media Gateway Control Protocol (MGCP) announcement (ANN) package, MLS provides announcement service via a remote MS. ThinkEngine Networks supports MGCP ANN; IPUnity does not.

Figure 6-22 illustrates the call flow for multi-lingual support.

Figure 6-22 Multi-Lingual Support Call Flow



The sections that follow provide additional information about MLS with ThinkEngine Networks, IPUnity, and IOS.

MLS with ThinkEngine Networks or IPUnity

1. A subscriber activates a feature (Call Forwarding on No Answer (CFNA), Direct Call Pick Up, etc.).
2. BTS terminates the call with a cause code.
3. BTS uses the terminating cause code to get the announcement number on the MS.
4. The announcement-number-prefix uses the mls-annc-mult-factor token from the MS Announcement table to create a new announcement number:

   announcement-number-prefix * ml-annc-mult-factor token + announcement id

   Without an mls-annc-mult-factor token, BTS uses default 1000. For example:

   English=1
   announcement-number-prefix=110
   multiplication factor=100000
   new announcement number=100110

   Spanish=2
   announcement-number-prefix=110
   multiplication factor=100000
   new announcement number=200110

   French=3
   announcement-number-prefix=110
   multiplication factor=100000
   new announcement number=300110

Note Use the number of announcements on the MS to set the mls-annc-mult-factor. If there are 1500 announcements on the MS, set the factor to 10000 not 1000.

5. BTS writes a message in a format specific to the MS type. For example the ThinkEngine Networks format is: **<a/>ann(<format>,<params>)**
   - **<format>**—MS vocabulary set, the syntax is **f(n)** where n starts at 1. Without format the default is **f(1)**. Vocabularies in the MS vocabulary slots match the language number on the BTS; if English = 1, load English vocabulary into MS slot 1.
   - **<params>**—MS actions, syntax is **pl(<list-of-params>**, repeat **rep(n,pl<list-of-params>**, where n=0 repeats forever

     For example the message telling the MS to play announcement 18 in:

     English=**S: A/ann(f(1),rep(1,pl(ps(18))))**
     Spanish=**S: A/ann(f(2),rep(1,pl(ps(18))))**
     French=**S: A/ann(f(3),rep(1,pl(ps(18))))**

Note ThinkEngine Networks sends the original announcement number in the parameter-list.

MLS with IOS

1. A subscriber activates a feature (Call Forwarding on No Answer (CFNA), Direct Call Pick Up, etc.).
2. BTS terminates the call with a cause code.
3. BTS matches the terminating cause code with a release cause code on the MS; this release cause code points to an announcement file from the announcement table.
4. BTS adds the announcement-file-prefix to the beginning of the announcement filename for IOS gateways:

   English file://welcome.wav is encoded to file://eng_welcome.wav
   Spanish file://welcome.wav is encoded to file://spa_welcome.wav
   for French file://welcome.wav is encoded to file://fra_welcome.wav

MLS Feature Interactions

There are some special interactions between the following features and MLS.

Remote Activation of Call Forwarding

Subscribers can pick a language for their Remote Activation of Call Forwarding (RACF) virtual number. After confirming the subscriber base number and Personal Identification Number (PIN), the IVR and announcements play in the selected language. If subscribers do not pick a language, IVR and announcements use default values.

No Solicitation Announcement

No solicitation announcement (NSA) is a terminating feature. MLS uses the language that the called party picks. For example: Subscriber B (calling party) picks Spanish. Subscriber A (called party) picks French and has NSA.

1. Subscriber B calls A.
2. Subscriber A's NSA activates.
3. Subscriber B hears French.

MLS Announcements

MLS adds a Spanish and French equivalent for each English announcement. Announcement IDs are the same for all languages.

Table 6-3 New MLS Announcements

Filename	Description	Suggested Wording
file:// welcome.wav	Plays a welcome tone.	Welcome
file://YouAreAbout.wav	Gives more information about the VSC.	You have accessed a menu to change your language of choice. If you know your choice, you may enter it at any time during this message.
file://Press.wav	Press (Atomic Segment)	Press
file://for.wav	For (Atomic Segment)	For
file://english.wav	English	English
file://spanish.wav	Spanish	Spanish
file://french.wav	French	French
file://youhaveselected.wav	The first audio segment played in the second IVR stage.	You have selected <var_audio>
file://asyourlanguageofchoice.wav	Provides your language of choice.	As your language of choice
file://toconfirmyourchoice.wav	Confirm choice.	To confirm your choice
file://toexitwithoutsaving.wav	Exit without saving choice.	To exit without saving your choice of language
file://yourlangaugeofchoiceisnow.wav	Confirm language of choice.	Your language of choice is now

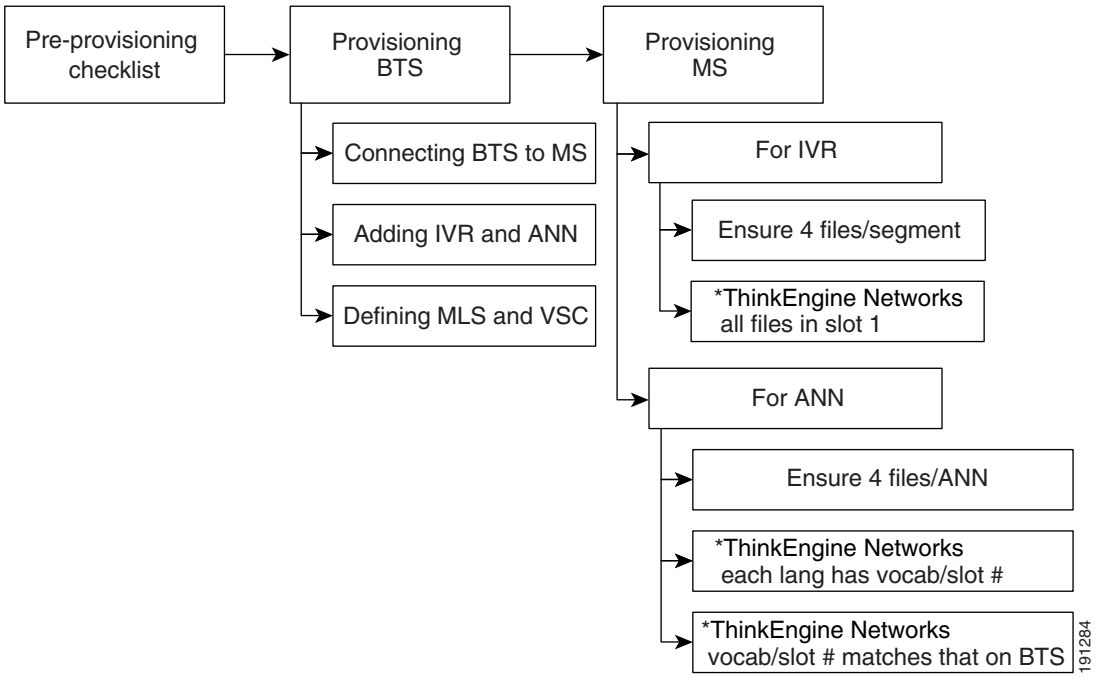
MLS Provisioning

Before starting the provisioning process, ensure that you have the following information.

- To install on the MS:
  - audio file names
  - audio file locations
- To set up the MS communication parameters:
  - IP addresses
  - voice port ranges
- To configure an IPUnity MS, know the announcement multiplication factor.
- To configure a ThinkEngine Networks MS, know the vocabulary installation order. Vocabularies in an MS vocabulary slots must match the language number on the BTS. If English=1, load English vocabulary into MS slot 1.

Figure 6-23 illustrates the provisioning flow for MLS.

Figure 6-23 Multi-Lingual Support Provisioning Flow



Provisioning the BTS 10200 for MLS

See the "Multi-Lingual Support for Interactive Voice Response and Announcements" section in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Provisioning the MS for IVR

IPUnity

Ensure there are 4 audio files for each IVR audio segment, 1 for each language and 1 for default.

ThinkEngine Networks

Ensure there are 4 audio files for each IVR audio segment, 1 for each language and 1 for default.

Install all IVR audio files in slot 1.

INDEX

Numerics

1-8XX numbers 1-5
211 numbers 1-7
311 numbers 1-7
411 numbers 1-7
500 personal communications services 1-6
511 numbers 1-7
611 numbers 1-7
700 service access calls 1-6
711 numbers 1-7
811 numbers 1-7
8XX calls
  processing outbound 1-14
8XX DNIS service 1-16
8XX numbers 1-6
900 numbers 1-6
911
  testing FGD-OS 1-60
911 overflow announcements 1-10
976 numbers 1-6

A

ABS 1-11
AC 3-75, 3-76
account codes 4-7
ACR 3-74, 3-75
activating 3-40, 3-46, 3-69, 3-71, 3-72, 3-75, 3-76, 3-78, 3-79, 3-82
  CFU 3-9
activating remotely 3-83
active call information display 1-16
active request limits 3-76
AIN FS 1-14
alarms 1-10
ALI 1-9
allowed CFC 3-31
allowed HOTV 3-82
alternate billing services 1-11
analog DID for PBX 3-58
ANI 1-3
ANI-based routing 1-3
ANI screening 4-10
anonymous call rejection 3-74
AR 3-76, 3-77
  with IVR 6-22
authorization codes 4-7
automatic callback 3-75
automatic location identification 1-9
automatic number identification 1-3
automatic recall 3-76

B

basic audio 3-110
basic business group 3-72
BAU 3-110
BBG 3-72
BGLs 3-73
billing office 1-8
Black/white list screening 1-16
black list 4-3
blocking
  call forwarding 3-8
  DNs by NOD 3-24
blocking flags 4-6

BLV 1-12
feature interactions 1-12
B-number 3-17
B-numbers 3-31, 3-82
allowed CFB 3-17
allowed CFC 3-31
bundling of features 3-135, 5-2
business group lines 3-73
busy line verification 1-12
busy line verification (BLV) 1-12

C

CA 1-5
CAC 1-11
CALEA 2-1
call 3-76
Call Agent 1-5
call barring options 4-1
call block 3-78
call center 1-16
caller ID 3-49
call forwarding 3-6
blocking 3-8
blocking DNs by NOD 3-24
maximums 3-6
call forwarding busy 3-16
call forwarding combined 3-31
call forwarding no answer 3-23
call forwarding unconditional 1-13, 3-7
call hold 3-69
calling
another country 1-4
another region 1-4
outside the EC, but in region 1-4
served by the same CO 1-3
within the same EC 1-3
calling card calls 1-11
calling identity 3-49
calling identity delivery 3-54
calling identity delivery blocking 3-51
calling identity delivery on call waiting 3-43
calling identity delivery suppression 3-54
calling identity presentation status 3-55
calling line identification presentation 3-50
calling line identification restriction 3-54
calling name delivery 3-49
calling name delivery blocking 3-53
calling number delivery 3-49
calling number delivery blocking 3-53
calling party number 1-19, 1-20
calling party number (CPN) 1-19, 1-20
call model 5-5
call park 3-71
call park subscriber group 3-71
call pickup without barge-in 3-72
call restrictions, screening 4-1
call retrieve 3-71
call return 3-76
calls
viewing active 1-16
call transfer 3-79
call waiting 3-39
call waiting deluxe activation 3-44
call waiting deluxe deactivation 3-45
cancel call waiting 3-42
carrier access code 1-11
CAS 1-9
casual dialing (dial around) 1-5
CBLK 3-78
CC 1-4, 3-8
CCW 3-42
activating 3-43
deactivating 3-43
Centrex features 3-68
CFB 3-16, 3-17
deactivating 3-20
feature interactions 3-22

CFBI 3-20
CFBL availability 3-20
CFBVA 3-17
customizing 3-17
CFBVD 3-20
CFC 3-31
allowed B-numbers 3-31
availability 3-34
conditions 3-31
feature interactions 3-38
subfeatures 3-34
VSCs 3-31
CFCI 3-34
CFNA 3-23
activating 3-26
availability 3-27
deactivating 3-27
feature interactions 3-29
CFNAI 3-27
CFNAVA 3-24
customizing 3-24
CFNA variable activation 3-24
CFNAVD 3-27
CFU 1-13, 3-7, 3-12
activating 3-9
availability 3-11
conditions 3-7
customizing 3-8
deactivating 3-10
CFUA
customizing 3-8
CFUD 3-10
CFVBBG 3-13
changing
calling numbers incoming 1-3
calling numbers outgoing 1-3
nature of address
DNISs 1-3
nature of address ANIs 1-3
channel-associated signaling 1-9
CHD 3-69
CIDB 3-51
CIDCW 3-43, 3-44
activating 3-44
deactivating 3-44
feature interactions 3-45
CIDSD 3-54, 3-57
CIDSS 3-54, 3-57
CLASS 3-1
class of service restrictions 4-1
CLEC 1-22
Click 2 Dial 1-30
CLIP 3-50, 3-51
CLIR 3-54, 3-55
CNAB 3-53, 3-56
CNAM 3-49
CND 3-49
CNDB 3-53, 3-56
collect calls 1-11
Communications Assistance for Law Enforcement Act 2-1
Community Information and Referral Services 1-7
community information and referral services 1-7
competitive local exchange carrier 1-22
compliance 3-82
conditions 3-17
COS 4-1
restrictions 4-2
COS restrictions 4-1
COT 3-80, 3-81
country code 1-4
courtesy call 3-8
CPN 1-19
CPRK 3-71
CPRK-RET 3-71
CPSG 3-71
CRCX 1-26
create-connection 1-26

CT 3-79
custom DNISs 1-16
customer-originated trace 3-80
customizing
CFUA 3-8
custom local area signaling service 3-1
Custom Ring-back Tone 1-30
CW 3-40, 3-41
CWD 3-45, 3-46
activating 3-47
associated features 3-46
conditions 3-46
deactivating 3-47
feature interactions 3-48
timers 3-46
CWDA 3-44
CWDD 3-45

D

DA/CWI 3-73
Data Rate Management Method 1-46
deactivating 3-41, 3-76, 3-77, 3-83
CFU 3-10
dedicated private line 3-81
default office service ID 3-134
delivery function server 2-2
denial announcement 3-76
denying subscribers service 3-119
DF server 2-2
dial-around service 1-22
dialed digits
collecting 1-5
reporting 1-5
dialed number identification service 1-3
Dialing number 1-3
dialing parity 1-22
dialing parity (intraLATA toll presubscription) 1-22
dialing plans 1-2
dialing procedures 1-2
Dialpad Sound Effects 1-30
dial plans
E.164 1-3
NANP 1-3
DID 3-58
DID for Centrex 3-72
Digit 1-2
Digit Manipulation 1-2
digit manipulation 1-3
digit pattern 1-5
DIGMAN 1-3
directed call pickup 3-72
direct inward/outward dialing for PBX 3-58
direct inward dialing for PBXs 3-58
directory assistance 1-7
direct outward dialing for PBXs 3-58
distinctive alerting/call waiting indication 3-73
distinctive ringing/call waiting 3-118
DN 1-3
DND 3-81
DNIS 1-3
DNIS-based routing 1-3
DNISs
changing NOA, ANIs
changing NOA 1-3
DOD 3-58
DOD for Centrex 3-72
do not disturb 3-81
DPN 3-72
DRCW 3-118
DTMF 1-6
DTMF relay 1-24
dual tone multifrequency 1-6

E

E.164
dial plan 1-3

E.164 dialing plan 1-2
E911 1-9
E911 tandem 1-9
easily recognizable codes 1-6
EC 1-3
EI 1-12
embedded multimedia terminal adapter 1-24
emergency calls 1-10
  provisioning 1-9
emergency functions (special) 1-9
emergency interrupt 1-12
Emergency Service Bureau 1-9
emergency service line 1-9
emergency services 1-8
emergency services (911) 1-8
eMTA 1-24
end-to-end called-party hold 1-9
Enhanced 911 1-9
Enhanced Voicemail UI 1-30
ENUM Capability 1-47
ERCs 1-6
ESB 1-9
ESL 1-9
Exchange code 1-3
external toll-free database 1-16

F

FCP 1-17
FDT 3-9, 3-36
  SIP interaction 3-36
Feature Control Protocol 1-17
feature interactions 3-12, 3-51, 3-69, 5-1
features
  inhibiting 5-9
Fill Bit Removal 1-45
final dial tone 3-36
final stage dial tone 3-9
forward-to phone number 3-17

G

GAP 1-23
Generic Address Parameter 1-23
group speed call 3-116

H

hotline 3-81
hotline-variable 3-82
HOTV 3-82, 3-83

I

IAP 2-2
ILEC 1-22
incoming SFG 3-68
incumbent local exchange carrier 1-22
Information digit-based screening 1-16
interactions 1-10, 5-1
interactive voice response 3-15
intercept access point 2-2
intercepting voice 2-2
intercept types
  Cisco SII 2-2
  PacketCable 2-2
international call forwarding 3-9
international number 1-4
INTL 3-9
intraLATA toll presubscription 1-22
ISFG 3-68
ITU-T CS-2 call model 5-1
IVR 3-15

J

JBIG Transcoding 1-46

L

LATAs 1-23
lawful intercept interface 2-1
LCO 1-26
limitations 3-81, 3-82
line testing 1-59
LNP 1-23
LNP functions 1-23
Local access and transport areas 1-23
local call 1-3
local connection option 1-26
local number portability 1-23
local number portability (LNP) 1-23
local toll call 1-4
local toll-free database 1-13
location routing number 1-23
long term denial announcement 3-76
LRN 1-23

M

main subscriber (MLHG 3-95
Maximum Bit Rate 1-45
maximum records stored 3-81
MCF 3-9
MDN 3-106
media gateway 1-5
Media-stimulated calling 1-6
Message Status 1-30
Message Waiting Indicator 3-89
MGW 1-5
Missed Call Status 1-30
MLHG 3-90
  circular hunt 3-91
  preferential hunts 3-93
  regular hunt 3-91
  sequence 3-90
  UCD 3-91
MMR Transcoding 1-46
MSC 1-6
MSOs 1-27
Multiline Hunt Group
  billing of calls 3-105
  main subscriber ID 3-95
  pilot DN 3-95
  provisioning account codes 3-95
  provisioning authorization codes 3-95
  provisioning speed call 3-95
multiline hunt group 3-90
Multiline Variety Package 3-105
Multi-party Voice Dialing 1-30
multiple call forwarding 3-9
multiple directory numbers 3-106
Multi-Ring Call Forward 1-30
Multi-Service Operators 1-27
MWI 3-89
  viewing status 3-90

N

NANPA audit compliance 1-8
national call restrictions 4-3
National destination code 1-3
national number 1-3
national prefixes 1-4
national toll call 1-4
nature of address 1-3
nature of dial 3-8
NDC 1-3
NEs 1-25
network elements 1-25
network features 1-1
next-free-terminal 3-91
NFT 3-91
NN 1-3
NOA 1-3
NOD 3-8

nonemergency information 1-7
no solicitation announcement 3-106
NPA 1-3
NRUF 1-8
NSA 3-106
  activating 3-107
  deactivating 3-107
  feature interactions 3-108
  IVR 6-24
numbering plan area 1-3
numbering plans 1-2
Numbering Resource Utilization and Forecast 1-8

O

OCB 4-1
  restrictions 4-2
office service ID 3-134
OI 1-12
  feature interactions 1-12
OLC 1-46
one-level 3-77
OOB 1-25
Open Logical Channel 1-46
operator callback 1-9
operator disconnect 1-9
operator interrupt 1-12
operator interrupt service 1-12
operator services 1-11
operator support
  international (CAC) 1-11
  international (PIC) 1-11
  local 1-11
  non-local 1-11
Originating test line 1-58
Origin-dependent routing 1-16
OSFG 3-68
OTL 1-58
outgoing call barring (OCB) 4-14
outgoing SFG 3-68
out of band 1-25
overflow announcements 1-10

P

PacketCable EMS/RADIUS interface 2-2
PAS 1-6
PBX 1-16
PCPS 3-55
PCS 1-6
per-call PS 3-55
Percentage-based routing 1-16
Permanent PS 3-52
person-to-person calls 1-11
PIC 1-11
pilot DN (MLHG) 3-95
PIN 3-111
PINs
  changing 6-5
PODP 1-23
PPS 3-52
prefixes
  provisioning restrictions 1-5
presentation status 3-55
presubscribed interexchange carrier 1-11
Privacy Screening 3-108
private identification number 3-111
provisioning 3-78
  features 5-2
  services 5-2
PS 3-55, 3-108
  feature interactions 3-113
  updates 3-113
PSAP 1-9
Public announcement services 1-6
public office dialing plan 1-23
public safety answering point 1-9

R

RACF 3-15, 6-2
  with IVR 6-2
radio station call-ins 1-6
RCF 3-16
reauthorization attempt 3-89
reject-caller 3-78
reminder ring 3-9
remote activation of call forwarding 3-15
remote call forwarding 3-16
repeat dialing 3-75
reporting
  DNs 1-8
  NRUF 1-8
restricting
  incoming calls 3-119
  outgoing calls 3-119
RFC 2833 support 1-24
RGW 1-17
routing
  based on ANI 1-3
  based on DNIS 1-3
RR 3-9

S

SAC 1-6
SCA 3-117
SCF 3-117
  IVR 6-7
SCP 1-13
SCR 3-78, 3-118
screening list editing 3-110
SDP 1-25
SDT 3-8, 3-35
  SIP interaction 3-36
Seasonal Suspend 3-59
second dial tone 3-35
second stage dial tone 3-8
selective call acceptance 3-117
selective call forwarding 3-117
selective call rejection 3-78, 3-118
service control point 1-13
Service Independent Intercept 2-1
Session Description Protocol 1-25
SFG 3-68
short term denial announcement 3-76
SII 2-1
simulated facility group 3-68
SLE 3-110
Smart Call Forward 1-30
Smart Call Return 1-30
SN 1-3
split NPA 1-38
storing records 3-81
subscriber features 3-1
subscriber number 1-3
subscribers
  denying services 3-119
surveillance 2-2
switch-based services 3-134

T

T.38 Fax Usage based on QoS Fax-t38-enabled Value 1-44
T108 test line 1-59
TCS 1-45
TDISC 3-119
  feature interactions 3-120
  restrictions 3-120
TDP 1-23
TDPs 5-1
teen service 3-106
telecommunications relay services 1-8
telephone repair service 1-7
Telephone voting 1-6

temporarily disconnected 3-119
Terminal and Group Make Busy Services 3-66
Terminal Capability Set 1-45
Terminating test line 1-58
testing
  911 FGD-OS trunks 1-60
  lines 1-59
  T108 test line feature 1-59
  trunks 1-58
TGW 1-9
three-way calling 3-121
three-way calling deluxe 3-122
Time-of-day routing 1-16
toll-free feature 1-13
Toll-free service call features 1-6
toll-free services 1-13
traffic information 1-7
trigger detection point 1-23
trigger detection points 5-1, 5-5
TRS 1-8
trunking gateway 1-9
trunk testing 1-58
trunk under test 1-59
TSAP 1-17
TTL 1-58
TUT 1-59
TV-Caller ID 1-30
TWC 3-121
  activating 3-122
  feature interactions 3-122
  limitations 3-121
TWCD 3-122
  timers 3-125
two-level 3-77

U

usage-sensitive three-way calling 3-127
USTWC 3-127
  limitations 3-127

V

vertical service codes 3-1
viewing
  active calls 1-16
VM 3-127
VMA 3-127
Voice Dialing 1-30
Voice Mail 3-127
Voice Mail Always 3-127
Voicemail Screening 1-30
Voice Menu 1-30
VSCs 3-1

W

warmline 3-134
white list 4-3
wiretap 2-1