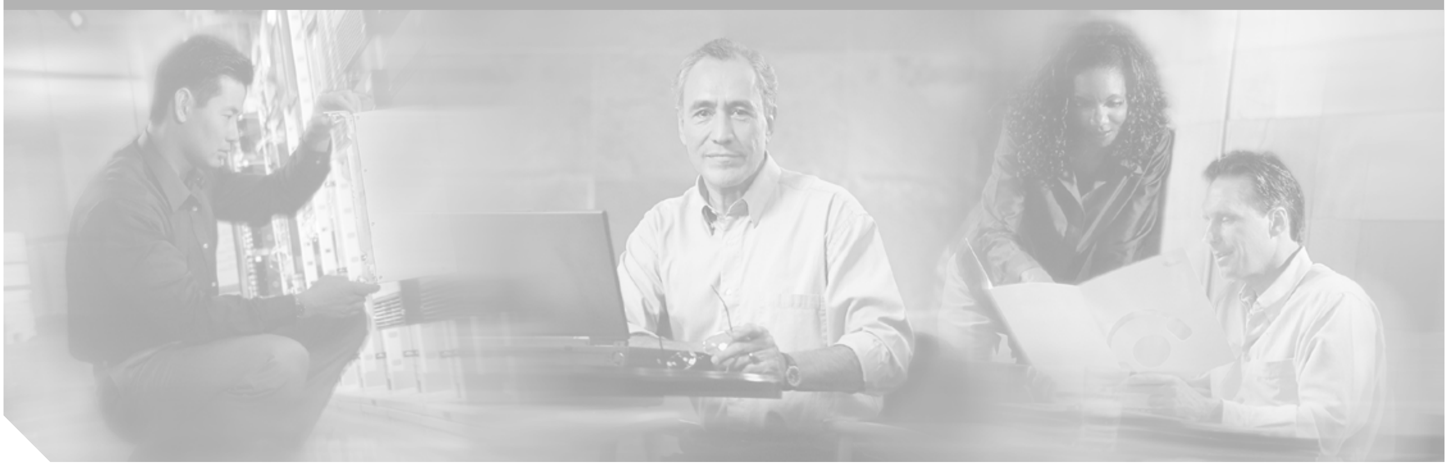
CISCO SYSTEMS



Cisco BTS 10200 Softswitch System Description, Release 4.4.x

Revised: March 19, 2007

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

Text Part Number: OL-5906-14

Cisco BTS 10200 Softswitch System Description, Release 4.4.x

CONTENTS

CHAPTER 6 **Feature Interactions**

Preface

Revised: March 19, 2007, OL-5906-14

This document provides an overview of the components, features, and functions of the Cisco BTS 10200 Softswitch. It describes the signaling protocols, network features, and subscriber features supported by the system.

Objective

The owner/operator of a Cisco BTS 10200 Softswitch can use this document to better understand how the system interfaces with their network, and how it provides network and subscriber features in conjunction with other network elements.

Audience

This document is designed for engineers, technicians, and system administrators who install, configure, and operate the Cisco BTS 10200 Softswitch.

Organization

This System Description contains the following chapters:

- Chapter 1, "Cisco BTS 10200 Softswitch Technical Overview"
- Chapter 2, "Supported Signaling Protocols"
- Chapter 3, "Network Features"
- Chapter 4, "Subscriber Features"
- Chapter 5, "Class of Service Restrictions and Outgoing Call Barring"
- Chapter 6, "Feature Interactions"

This document also includes a glossary and an index.

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.

Revision History for Release 4.4.x

This document includes all of the information that was contained in the previous issue (the Release 4.1 System Description), and has been updated for Release 4.4.x as described in this Preface.

Note All of the features and functions described in this document are applicable to both Release 4.4.0 and Release 4.4.1, unless specifically noted. Release 4.4.x refers to both Release 4.4.0 and 4.4.1.

The following list is a summary of features that are specific to Release 4.4.1, and are not supported in Release 4.4.0. See the appropriate documents in the Release 4.4.x documentation set:

- OCB enhancements (See the *Cisco BTS 10200 Softswitch Enhanced Outgoing Call Barring Feature Module*)
- ETSI v2 ISUP variant. (See the *Release Notes* for a list of ISUP variants supported for specific countries.)
- ISDN updates (See the *Cisco BTS 10200 Softswitch ISDN Provisioning and Troubleshooting Guide*):
  - ETSI Net 5 PRI
  - User Side Support of ISDN PRI
  - ISDN Info Digits
- H.323 applications (See the *Cisco BTS 10200 Softswitch H.323 Protocol Guide*)
- Short term LNP requirement (See the *Cisco BTS 10200 Softswitch Release Notes* document)

Following is a summary of the major changes and additions to this Release 4.4.x document versus the Release 4.1 document:

- Chapter 1, "Cisco BTS 10200 Softswitch Technical Overview":
  - Described the new interface configuration with four Ethernet interfaces on the CA and two on the EMS. The four interfaces on the CA allow separation of system management data from external signaling and communications data.
  - Added a statement that the Mini-Browser Adapter (MBA) runs on a separate host machine.
  - Referred to the *Release Notes* document for a list of hardware options on which the Cisco BTS 10200 Softswitch software can run.
  - Added information about the CLI-based dialed-number query tools, QVT and TVT.

- Updated information regarding DNS and IP Manager.
- Added information about new system security features for Release 4.4.x.
- Added information about AUEP and ICMP pings for MGCP-based MGWs.
- Added or modified wording to improve organization and clarity (throughout).

- Chapter 2, "Supported Signaling Protocols"
  - Updated the description of the ISDN capabilities.
  - Removed information on PacketCable and H.323 protocols that is available in protocol-specific documents (*Cisco BTS 10200 Softswitch PacketCable Guide* and *Cisco BTS 10200 Softswitch H.323 Protocol Guide*).
  - Added a line regarding SIP-trunk route advance feature.
  - Removed reference to M3UA layer.
  - Version OL-5906-08—Updated the list of supported ISUP variants.
- Chapter 3, "Network Features":
  - Updated information on T.38 fax transmission modes (feature enhancement in Release 4.2).
  - Added information on calling party number (CPN) options (Release 4.2 feature).
  - Added information about the simultaneous operation of both PacketCable Intercept mode and Cisco SII mode for CALEA.
  - Added information on the basic network loopback testing feature.
  - For version OL-5906-09, the following changes were made:

    EMG/911—Interaction with CHD was added.

    BLV/OI—Information was added for interaction with CFU (when CFU activated), and interaction with all other features (when invoked). Information was added on provisioning the denial of BLV function per subscriber.
  - For version OL-5906-12, the following changes were made:

    Enhanced the description of "Calling Party Number Options for Outgoing SETUP Messages."

    Enhanced the description of "n11 support (211, 311, 411, 611, 711, 811)" and included support for 211 calls.
  - Version OL-5906-13, the following changes were made:

    Clarified the description of the 8XX (Toll-Free Calling) feature.
- Chapter 4, "Subscriber Features":
  - Added information on the two-step automatic recall (AR) function.
  - Added statement that CFB features are applied when a subscriber line is unreachable.
  - Updated description of ACR activation.
  - Version OL-5906-07—Added limitations and interactions information:

    - Added information on limitations for using certain features (CW, CIDCW, TWC and USTWC) when using ISUPs other than ANSI ISUP.

    - Added information specific to Centrex users with CHD feature—There are limitations on call forwarding when CHD, CFNA, and CW are all active on the subscriber line.

- Version OL-5906-08—Deleted an incorrect statement regarding the Call Transfer (CT) feature. The deleted (incorrect) statement said that CT is available only to Centrex subscribers. The correct statement is that CT is available to both POTS and Centrex subscribers.
- Version OL-5906-09, the following changes were made:

  CFU—Interaction with BLV/OI was added.

  CHD—Interaction with EMG/911 call was added.
- Version OL-5906-10, the following changes were made:

  CT/TWC and CT/TWCD interactions—Additional details about these interactions were added.

  CW/CFNA interaction—Additional details about this interaction were added.

  CW, CIDCW, and CWD—VSC examples were updated.

  CW and CIDCW—The paragraphs about limitations and feature interactions was moved within these sections, but no content changes were made.
- Version OL-5906-11, the following change was made:

  Update to the CFB description—Added a note regarding limitation on call forwarding when subscriber is unreachable.
- Version OL-5906-13, the following changes were made:

  Added a note regarding CCW behavior if there is a CA switchover.

  Clarified the description of the MLHG feature.
- Version OL-5906-14:

  Additional clarifications were added regarding MLHG.

- Chapter 5, "Class of Service Restrictions and Outgoing Call Barring":
  - Added information on the provisionable timers for account codes and authorization codes used with the COS restriction feature.
  - Made corrections and clarifications to the COS flow diagrams.
  - Added a reference to the *Enhanced Outgoing Call Barring* Feature Module for Release 4.4.1.
- Chapter 6, "Feature Interactions":
  - Version OL-5906-09—Information was added to show that CT has precedence over both TWC and TWCD.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- *The Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/go/packet
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

Cisco BTS 10200 Softswitch Technical Overview

Revised: March 19, 2007, OL-5906-14

This chapter provides a summary of the features and functions of the Cisco BTS 10200 Softswitch. The following topics are discussed in this chapter:

- Introduction
- Cisco BTS 10200 Softswitch in the TMN Model
- Overview of Features and Functions
- Logical Components
- Cisco Specified Hardware
- Site Preparation

Note All of the features and functions described in this document are applicable to both Release 4.4.0 and Release 4.4.1, unless specifically noted. Release 4.4.x refers to both Release 4.4.0 and 4.4.1.

Introduction

The Cisco BTS 10200 Softswitch is a software-based, class-independent network switch. It provides call-control intelligence for establishing, maintaining, routing, and terminating voice calls through the packet network via media gateways (MGWs), while seamlessly operating with legacy circuit-switched networks. In VoIP networks it processes incoming and outgoing calls between the packet network and the public switched telephone network (PSTN). The Cisco BTS 10200 Softswitch provides the major signaling functions performed by traditional Class 4 and Class 5 switching systems in the PSTN. It also provides more than 40 provisionable subscriber features, and management interfaces for provisioning, monitoring, control, and billing operations.

Note The bearer path infrastructure is provided via MGWs, which interface circuit-switched facilities with packet networks. The MGWs provide encoding/decoding and packetization/depacketization functions.

When Cisco BTS 10200 Softswitch application software is installed on Cisco specified host machines, it creates a set of logical components. Together these logical components provide all of the features and functions of the Cisco BTS 10200 Softswitch. The disk drives in the host machines store the provisioned database and system-generated data. These logical components, and the Cisco specified hardware, are described later in this chapter.

The Cisco BTS 10200 Softswitch communicates with a wide range of network elements (NEs) including

- Service provider network management and support systems
- Gateways to managed packet networks and PSTN
- NEs that support network and subscriber services such as billing mediation and record keeping, interactive voice response (IVR), announcements, law enforcement and emergency services, operator services, and so forth.

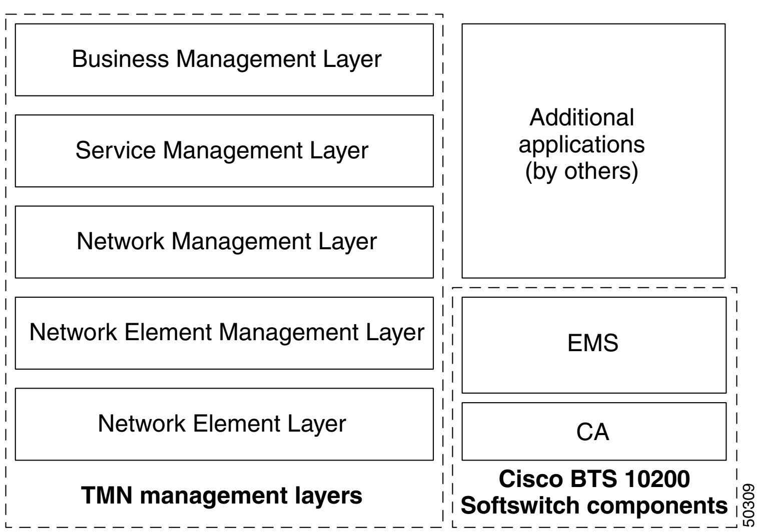
When ordering the Cisco BTS 10200 Softswitch software, your Cisco account team will work with you to determine appropriate hardware options, software loads, and license level options for each of your sites.

Note License level options involve the number of subscribers/DS0 lines and calls per second (CPS). You can order increased subscriber/DS0 and CPS license levels from your Cisco account team.

Cisco BTS 10200 Softswitch in the TMN Model

Figure 1-1 illustrates the role of the Cisco BTS 10200 Softswitch in the Telecommunications Management Network (TMN) model. The Cisco BTS 10200 Softswitch is involved in the Network Element Layer and Network Element Management Layer.

Figure 1-1 Cisco BTS 10200 Softswitch Components in the TMN Model



Note The Call Agent (CA) and Element Management System (EMS) components of the Cisco BTS 10200 Softswitch, as shown in Figure 1-1, are described in the "Logical Components" section on page 1-8.

The role of each TMN layer is described below.

The Business Management Layer contains the following elements:

- Network planning
- Intercarrier agreements
- Strategic planning
- Enterprise-level management

The Service Management Layer contains the following elements:

- Customer interface
- Service provisioning
- Account management
- Customer-complaint management
- Integrated faults, billing, and quality of service (QoS)

The Network Management Layer contains the following elements:

- End-to-end network view
- All data aggregated to the network view
- Physical entity awareness

The Network Element Management Layer contains the following elements:

- Subnet management
- Element management
- Reduced workload on the Network Management Layer
- Common NEs aggregated in a network

The Network Element Layer contains the following elements:

- Performance data generation
- Self-diagnostics
- Alarm monitoring and generation
- Protocol conversions
- Billing generation

Overview of Features and Functions

The Cisco BTS 10200 Softswitch provides a large number of features and functions. This section contains quick-reference lists of the features and functions in the following categories:

- Network Features and Functions
- Subscriber Features
- Billing Features and Functions
- Operations, Maintenance, and Troubleshooting Features and Functions
- System Administration Features and Functions

Tip This list is intended as a general overview. Additional features and functions are described within the complete documentation set for this product.

Network Features and Functions

The system supports the following network features and functions:

- Call control intelligence for establishing, maintaining, routing, and terminating voice calls through the packet network via media gateways (MGWs), while seamlessly operating with circuit-switched networks.
- Support for a number of network signaling protocols, including MGCP, SIGTRAN (for SS7), H.323, PacketCable, Session Initiation Protocol (SIP), ISDN, and channel-associated signaling (CAS).
- PSTN-parity routing mechanisms for voice calls including local, national, international, operator services, and emergency services routing. (In North America, this includes local access and transport area (LATA) calls and interLATA calls.)
- Support for the following types of calls:
  - PSTN-to-Packet Network calls—Calls that originate on a PSTN network and terminate on a packet network (off-net calls).
  - Packet-to-PSTN Network calls—Calls that originate on a packet network and terminate on a PSTN network (off-net calls).
  - Packet-to-Packet calls—Calls that originate and terminate on a packet network (packet on-net calls).
  - PSTN-to-Packet-to-PSTN calls—Calls that originate on an ingress PSTN circuit and travel over a packet network to terminate on an egress PSTN port.
- Support for the following types of routing, configurable via command-line provisioning:
  - Trunk-based routing, with trunk group (TG) selection options as follows: least-cost routing, round robin, or sequential order.
  - Policy routing, including origin-dependent routing, originating line information (OLI) routing, percent routing, point of presence (POP) routing, prefix-based routing, region-based routing, time-of-day routing, and NXX-based routing.
  - Equal access routing.
- Support for route advance—The route table in the Cisco BTS 10200 Softswitch database allows the service provider to provision a list of up to 10 trunk groups (TG1 to TG10), and a parameter for selecting the priority of the TGs for routing (TG-SELECTION). The system attempts to route the call on the highest priority TG. If the call cannot be completed on the highest priority TG, the system attempts to use the next (lower priority) TG, a process known as route advance. The system attempts route advance to lower priority TGs up to five times. (Any TG in the list that is administratively out of service is not counted as an attempt.) If all five attempts fail, the call is released, and the system provides a release announcement.
- Digit manipulation function, which enables the Cisco BTS 10200 Softswitch to modify the calling party dial number, called party number, and nature of address (NOA) for both incoming and outgoing calls. This feature supports the use of:
  - North American Numbering Plan (NANP).
  - ITU-T E.164 numbering plan.

  - ANI- or DNIS-based routing.

> **Note** The calling party number is also known as ANI (automatic number identification), and the called party number is also known as DNIS (dialed number identification service).
>
> NOA values include international number, national number, operator call, subscriber number, test line, unknown, and up to six network-specific designations.

- Support for domestic and international equal-access direct dialing based on presubscribed interexchange carrier (PIC).
- Support for provisionable Common Language Location Identifier (CLLI) codes:
  - Provides identification of the local switch (Cisco BTS 10200 Softswitch) and the remote switch (the switch at the far end of the applicable trunk group).
  - Supports sending and receiving CLLI code in circuit validation response (CVR) messages—CVR messages are generated in response to a circuit validation test (CVT) message.
- Control of announcement servers.
- Communications with interactive voice response (IVR) servers.
- SIGTRAN-based communications with signaling gateways (SGs) that provide SS7 signaling and interoperability with legacy PSTN equipment.
- Interoperability with PBX equipment via ISDN-PRI and channel-associated signaling (CAS) protocols.
- Generation of triggers allows service providers to offer enhanced services using external service platforms (consistent with the ITU CS-2 call model).
- Enhanced Centrex services (virtual office) for business subscribers, including telecommuters and mobile workers.
- Dial offload—Dial offload involves intercepting Internet traffic at inbound Class 5 locations and carrying this traffic over the packet network (instead of the PSTN) to the Internet service providers (ISPs).
- Call control functions for the H.323-based gateways and endpoints.
- Support for H.323 Annex E User Datagram Protocol (UDP) functionality, which preserves stable calls during a process restart or component switchover on the CA.
- Interworking with Cisco CallManager using H.323 protocol.
- Call control functions for Tandem applications.
- Call control functions for SIP-enabled networks.
- Call control functions for PacketCable-based networks, including support for Common Open Policy Service (COPS), Network-Based Call Signaling (NCS) protocol, and Trunking Gateway Control Protocol (TGCP) signaling, as well as IPsec and dynamic quality of service (DQoS) features.
- T.38 fax relay.
- Public safety answering point (PSAP) support for Enhanced 911 Emergency Services.
- Interfaces for support of the Communications Assistance for Law Enforcement Act (CALEA), in both PacketCable and Cisco Service Independent Intercept (SII) architectures.
- Support for the automatic call gap (ACG) function with service control point (SCP) query.

Subscriber Features

The system supports the following subscriber features:

- Call processing, subscriber services and features, billing support and carrier class availability/reliability for subscribers and trunks connected to media gateways.
- A large number of voice-handling features, such as call waiting, call holding, call transferring, multiline hunting and caller identification (see the other chapters in this document for complete coverage).
- Class of service (CoS) screening and outbound call barring (OCB).

Billing Features and Functions

The system supports the following billing features and functions:

- Provisionable option for FTP or SFTP transfer of call data to a remote billing server or third-party billing mediation device.
- User-provisionable billing collection and transfer parameters.
- User-configurable billing reporting by call type.
- Option for call detail block (CDB) or event message (EM) billing data formats.

Note See the *Cisco BTS 10200 Softswitch Billing Interface Guide* for a complete description of the billing functions.

Operations, Maintenance, and Troubleshooting Features and Functions

The system supports the following operations, maintenance, and troubleshooting features and functions:

- Hardware sizing options appropriate for a variety of traffic types and call rates.
- Redundant hardware and software fail-safes to provide reliable operation and minimize the chance of an outage.
- Support for regular database backup, and recovery of data from backup files.

  Note Data should be backed up on a daily basis and saved to a remote server. Data backup files are needed in the unlikely event that data in both the primary and secondary sides of any platform become corrupted. In that case, the data must be restored from a backup file.

- Periodic and scheduled audits of circuits to detect and clear “hung” circuits. Audits are performed on:
  - SS7 circuits
  - MGCP trunking gateway circuits
- Command-line based dialed-number query tools:
  - A query verification tool (QVT)—This tool generates Transaction Capabilities Applications Part (TCAP) queries to the SCP database, and reports query results.

  - A translation verification tool (TVT)—This tool determines the routing for a call by traversing through the tables provisioned in the database without originating any call.
- Traffic measurements, such as call-completion counters, resource status and congestion information.
- Event and alarm reports, including user provisioning of report filters.
- Congestion detection and protection feature, with the following characteristics:
  - Detects internal messaging congestion caused by traffic overload or other extraordinary events, and takes preventive action to avoid system failure.
  - When the Cisco BTS 10200 Softswitch is in a congested state, emergency messages are given special treatment and are allowed to pass through.
- Provisionable option to suppress sending of Internet Control Message Protocol (ICMP) ping—The service provider can enable or disable sending ICMP pings to MGWs. (The Cisco BTS 10200 Softswitch sends an ICMP ping only when an audit-endpoint [AUEP] attempt fails.)

System Administration Features and Functions

The system supports the following system administration features and functions:

- Secure communications using SSH, SFTP, Secure XML, and HTTPS interfaces.
- Hardened Solaris OS—The Cisco BTS 10200 Softswitch runs on Sun Solaris. Processes and utilities in the UNIX system that are unsuitable for use in a softswitch environment have been disabled.
- Login authentication—The Cisco BTS 10200 Softswitch supports administrative login authentication using Lightweight Directory Access Protocol (LDAP) and RADIUS authentication clients. This functionality is applicable to the Cisco Extensible Provisioning and Operations Manager (EPOM) and Cisco Self-Service Phone Administration (SPA). The system can determine if the account is local or off-board, and transfer login responsibility for off-board accounts to the end-user authentication, authorization, and accounting (AAA) servers. This capability is provisionable via command-line interface (CLI) commands.
- Common Object Request Broker Architecture (CORBA) Adapter (CAD) interface—The CAD provides an abstraction of the Cisco BTS 10200 Softswitch in a consistent, object-oriented model. The CAD interface supports a means of provisioning the Cisco BTS 10200 Softswitch that parallels the CLI adapter capabilities. The system provides a secure socket layer (SSL) transport for the CORBA adapter.

Note For CORBA details, see the *Cisco BTS 10200 Softswitch CORBA Adapter Interface Specification Programmer Guide*.

- A provisionable database containing data for basic call processing, billing, and special call features.
- Communication with the existing Operations Support System (OSS) infrastructure—including network management systems (NMSs)—to support fault, configuration, accounting, performance, and security (FCAPS) functions.
- Communication with the Cisco SPA—Cisco SPA uses a web-based interface for feature self-provisioning and account management that can be used by consumers, account holders, and service providers. It enables the end user to manipulate existing features and query account information without service provider intervention or labor.

Note The SPA function requires additional hardware—It does not run on the Cisco BTS 10200 Softswitch hardware platform.

Logical Components

This section discusses the logical components of the Cisco BTS 10200 Softswitch and describes the functions of each component. The information is organized as follows:

- List of Logical Components
- CA Functions
- FS Functions
- EMS Functions
- BDMS Functions
- MBA Functions
- Reliability and Availability of Components

List of Logical Components

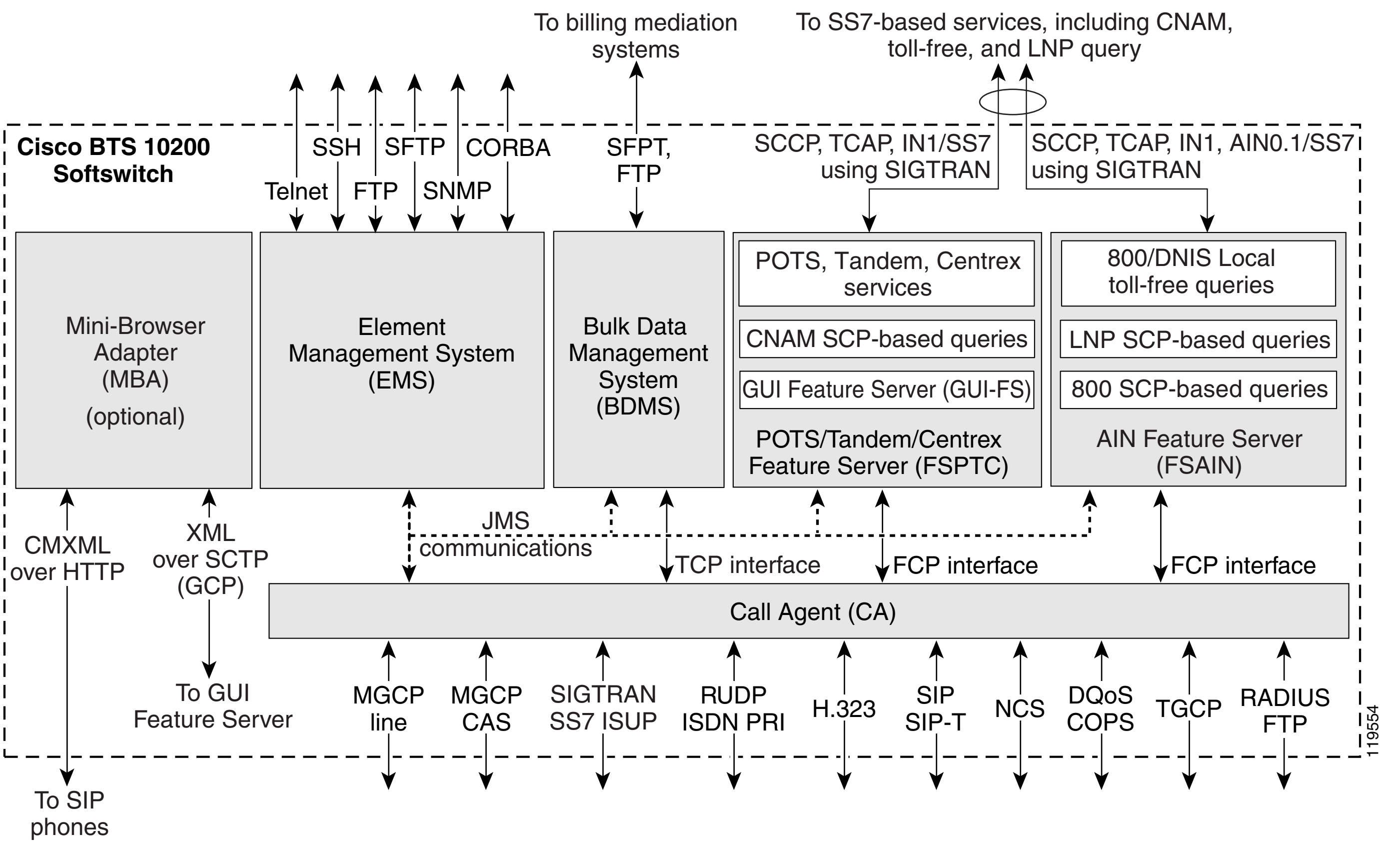
The Cisco BTS 10200 Softswitch consists of five independent logical components in a distributed architecture:

- Call Agent (CA)—Serves as a call management system and media gateway controller. It handles the establishment, processing, and teardown of telephony calls.
- Feature Servers (FSs)—Provide POTS, Tandem, Centrex, and Advanced Intelligent Network (AIN) services to the calls controlled by the CAs. The FSs also provide processing for service features such as call forwarding, call waiting, local number portability, and so forth.

  There are two types of FSs in the Cisco BTS 10200 Softswitch:
  - FSPTC—FS for POTS, Tandem, and Centrex features
  - FSAIN—FS for AIN services
- Element Management System (EMS)—Controls the entire Cisco BTS 10200 Softswitch, and acts as a mediation device between a network management system (NMS) and one or more CAs. It is also the interface for the provisioning, administration, and reporting features of the Cisco BTS 10200 Softswitch.
- Bulk Data Management System (BDMS)—Coordinates the collection of billing data from the CA, and the forwarding of billing records to the service provider billing mediation device.
- Mini-Browser Adapter (MBA)—Performs GUI management for GUI-enabled SIP phone handsets. This GUI allows SIP phone users to self-provision certain features. The MBA runs on a separate Sun host machine that is not part of the standard Cisco BTS 10200 Softswitch hardware set.

The architecture and interworking of the logical components (CA, FS, EMS, BDMS, and MBA) are shown in Figure 1-2. The detailed functions of each component are described in the sections that follow.

Figure 1-2 Cisco BTS 10200 Softswitch Architecture, Showing Logical Components



Notes for Figure 1-2:

The MBA runs on a separate Sun host machine that is not part of the standard Cisco BTS 10200 Softswitch hardware set.

The minimal/earliest CMXML version supported for communications between the MBA and SIP phones is CMXML 3.0.

CA Functions

The Call Agent (CA) provides monitoring and control of external NEs. It connects to multiple networks via the signaling adapter interface. This interface converts incoming and outgoing signaling to and from the standard internal format of the CA. This interface allows the CA to connect to multiple networks and exchange signaling messages for setup, teardown, and transfer of calls.

Signaling Adapters

The signaling adapters perform the following functions:

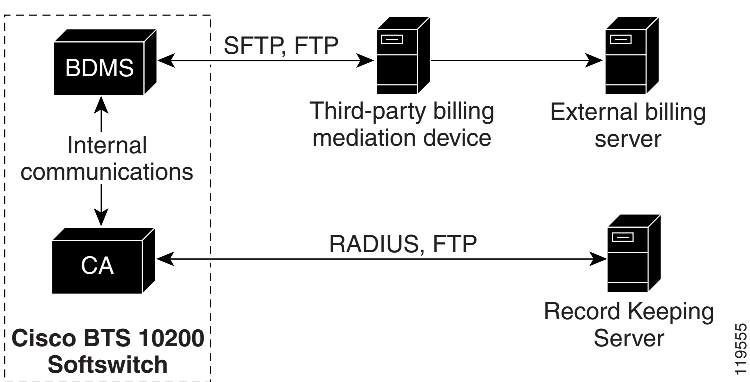
- Provide uniform primitives (signaling indications) for all interactions between different protocol stacks and the CA modules.
- Provide uniform data structures containing common information elements from different signaling protocols.
- Provide call control primitives for exchanging all call signaling messages between CA and the signaling network.
- Provide maintenance primitives for signaling link hardware maintenance and signaling protocol stack provisioning.

Billing Data Generation and Interfaces

The CA supports the following billing data generation methods:

- Call detail blocks (CDBs)—This is traditional post-call billing data, which the CA sends via internal communications to the BDMS (see Figure 1-3). The BDMS forwards this data via FTP or SFTP (a provisionable option) to a third-party billing mediation device. For additional information on the BDMS, see the "BDMS Functions" section on page 1-15.
- PacketCable event messages (EMs)—This is real-time call data flow, which is transferred directly from the CA to an external Record Keeping Server (RKS) that assembles call detail records (CDRs) from the EMs. The following billing interfaces are provided for EMs on the CA (see Figure 1-3):
  - Remote authentication dial-in user service (RADIUS)—Used by the CA to transmit EMs automatically to an external RKS
  - FTP—Used for manual transfer of EMs from the CA to the RKS

Figure 1-3 CA Billing Interfaces



Caution Cisco strongly recommends that you do not provision the system to generate CDBs and EMs simultaneously. Attempting to generate both types of records simultaneously can significantly degrade system performance.

Note FTP sessions are used for file transfers initiated by the Cisco BTS 10200 Softswitch.

FS Functions

There are two different types of Feature Servers (FSs) in the Cisco BTS 10200 Softswitch.

- FSPTC—FS for POTS, Tandem, and Centrex features
- FSAIN—FS for Advanced Intelligent Network services

Each FS communicates internally with the CA, and externally (via a signaling gateway) with STPs that are part of the SS7 signaling system.

The FSs provide access to features through a well-defined interface. The Cisco BTS 10200 Softswitch architecture logically separates the FSs (which provide feature control) from the CA (which provides call control) with a clear interface—Feature Control Protocol (FCP)—defined between them. The FSs provide support for POTS, Centrex, AIN, 8XX service, and other enhanced services. The FSs are colocated on the same machine as the CA.

An FS is invoked from a call detection point (DP) in the CA. For each DP, the CA checks if any triggers are armed. If a trigger is armed, the CA checks if the trigger applies to the subscriber, group, or office (in that order). If the trigger is applicable, the CA invokes the FS associated with that trigger. The Cisco BTS 10200 Softswitch call processing mechanisms are based on the ITU CS-2 call model. For DP details, see the *Cisco BTS 10200 Softswitch Operations Manual*.

The FSAIN supports the automatic call gap (ACG) function for communications with a service control point (SCP). When an SCP sends a message to the FSAIN regarding the allowed query rate, the Cisco BTS 10200 Softswitch adjusts its query rate accordingly.

EMS Functions

The Element Management System (EMS) manages all of the Cisco BTS 10200 Softswitch components and provides operations, administration, maintenance, and provisioning (OAM&P) interfaces for monitoring and control. It provides the following user OAM&P capabilities:

- Access the system via a secure interface.
- Perform system administration and security functions.
- Show, add, change, or delete the database information through a local or remote interface.
- Display reports of events, alarms, and faults.
- Monitor and manage hardware.
- Monitor and manage traffic measurements.
- Monitor and manage queuing and audit functions.
- Display and control the status of a component.

The internal database contains the provisioned data for basic call processing, billing, and special call features. Key data structures are stored in shared memory and are accessible to any process in the system. A library of read/write locks controls access to shared memory. The data structures are implemented using Oracle in the EMS/BDMS, and an indexed database (IDX) in the CA/FS.

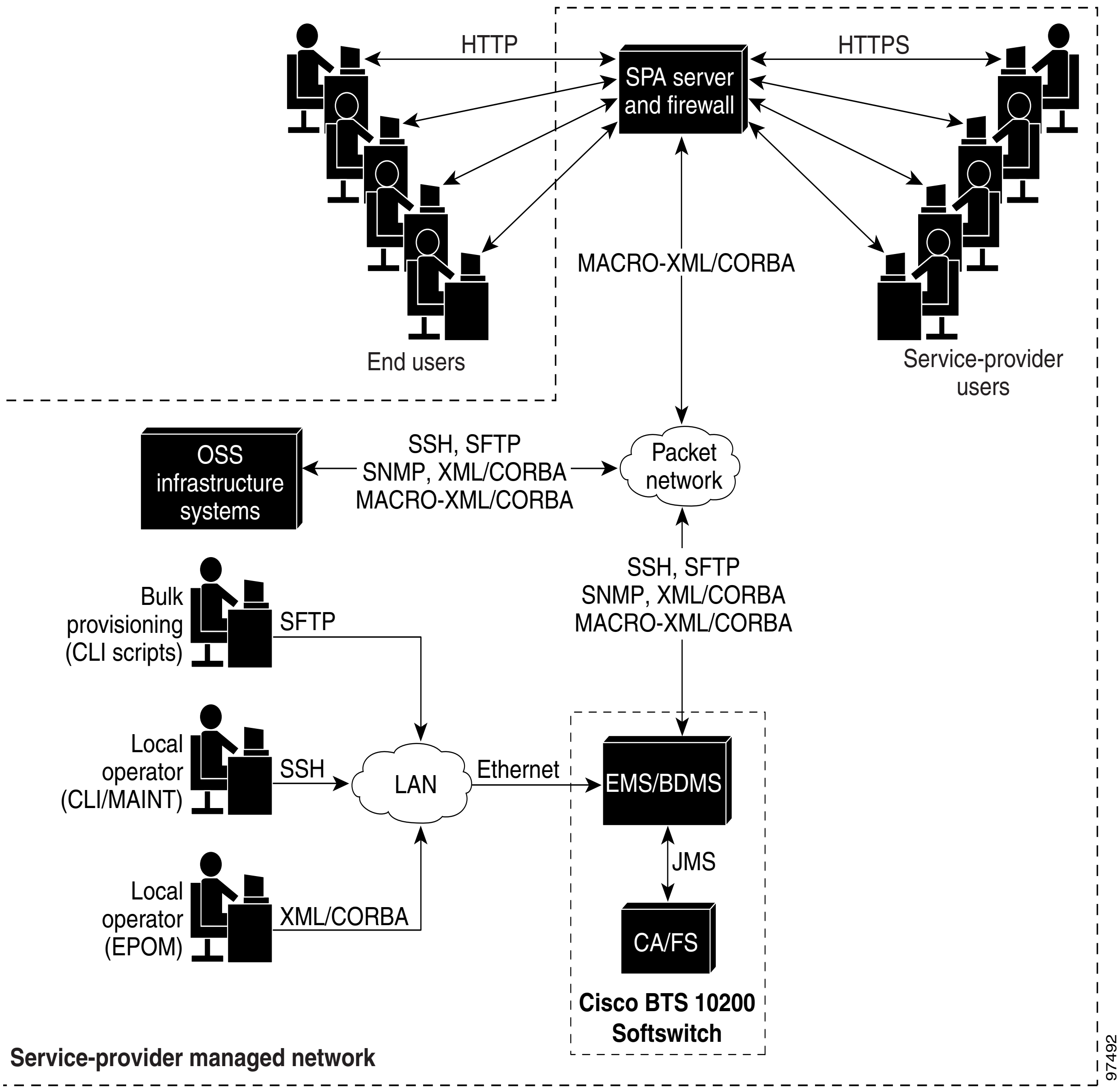
Note For additional information on using these functions, see the *Cisco BTS 10200 Softswitch Operations, Maintenance, and Troubleshooting Guide*, the *Cisco BTS 10200 Softswitch Provisioning Guide*, and the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide.*

The EMS provides a flexible mechanism to transport information over any protocol to any external device. The EMS interface design takes into account that each carrier has its own unique set of Operations Support Systems (OSSs). The EMS provides a decoupling layer between the external protocols used within the service provider network and the internal protocols of the Cisco BTS 10200 Softswitch. The core system does not need to interpret the specific data formats used by the other carrier network elements.

EMS Communications

Operators, network administrators, and end users can communicate with the EMS from their workstations or PCs over the interfaces shown in Figure 1-4.

Figure 1-4 Preferred EMS Management Interfaces for Service Provider and End Users



The user interfaces include the following:

- Secure shell (SSH)—For provisioning via CLI and Maintenance (MAINT) shells.
  - CLI shell—Used for entering entire commands and their parameters from the command line.
  - MAINT shell—Provides a maintenance interface for CLI commands that does not time out or disconnect on switchover. It supplies a prompt based on the username.

> **Note** After software installation, you must enable CLI provisioning by applying database licenses. You will not be able to run CLI commands until this is done. Your Cisco account team can provide the necessary licenses and procedures.

- Secure File Transfer Protocol (SFTP)—For bulk provisioning sessions. SSH and SFTP are always available on the Cisco BTS 10200 Softswitch, and there is no command to turn them off.

> **Note** For security purposes, Telnet is no longer supported as of Release 4.4.x.

- XML/CORBA and MACRO-XML/CORBA support the following:
  - CORBA provisioning and monitoring interface
  - Provisioning via the Cisco Extensible Provisioning and Operations Manager (EPOM) and the Cisco Self-Service Phone Administration (SPA)

> **Note** MACRO-XML/CORBA is a read-only interface that end users can configure and use to display large sets of data. It is used to streamline data queries and display complex data relationships.

  - CORBA over SSL for communications with the Cisco BTS 10200 Softswitch
- Simple Network Management Protocol (SNMP)—Provides traps, status, control, and measurement functions, and provisionable community strings
- Hypertext Transfer Protocol (HTTP) and Secure Hypertext Transfer Protocol (HTTPS)—Permits end users and service providers to perform many of the feature provisioning processes via the web-based Cisco SPA system. Access from the user's web browser to the SPA server is via HTTP. Access from the service provider's web browser is via HTTPS.

By default, SFTP sessions are used for file transfers initiated by elements outside the Cisco BTS 10200 Softswitch (and directed toward the Cisco BTS 10200 Softswitch). FTP sessions are used for file transfers initiated by the Cisco BTS 10200 Softswitch.

> **Note** The functions of the BDMS component, including billing-related communications links, are described in the "BDMS Functions" section on page 1-15.

SNMP Agent

The following functions are supported by the Cisco BTS 10200 Softswitch SNMP Agent:

- Collection of statistics and traffic management data
- Status and control
- SNMP trap reports
- Bulk Status and control

The SNMP agent supports SNMPv2c operations defined by the opticall.mib Management Information Base (MIB). The MIB is located in the directory /opt/BTSsnmp/etc on the EMS. The NMS needs to load the main MIB (opticall.mib), that will in turn import three other MIBs— IPCELL-TC, SNMPv2-TC, and SNMPv2-SMI. The main MIB uses variables from these other three MIBs.

BDMS Functions

The Bulk Data Management System (BDMS) stores billing data in the form of call detail blocks (CDBs). CDBs are assembled from billing messages generated in the CA when billing-related call events occur during call processing. The BDMS formats the CDBs into a flat ASCII-file format, and transmits them to an external billing collection and mediation device that is part of the service provider billing system (see Figure 1-5). Finally, the BDMS forwards this data to an external billing mediation system or billing server, where it is assembled into CDRs.

Note The interface to the billing mediation device can vary from carrier to carrier. The BDMS supports a flexible profiling system that allows the Cisco BTS 10200 Softswitch to adapt to changes in the billing mediation device interface. The BDMS transmits billing records via FTP or SFTP to the mediation device at regular time intervals that are provisionable in the Cisco BTS 10200 Softswitch.

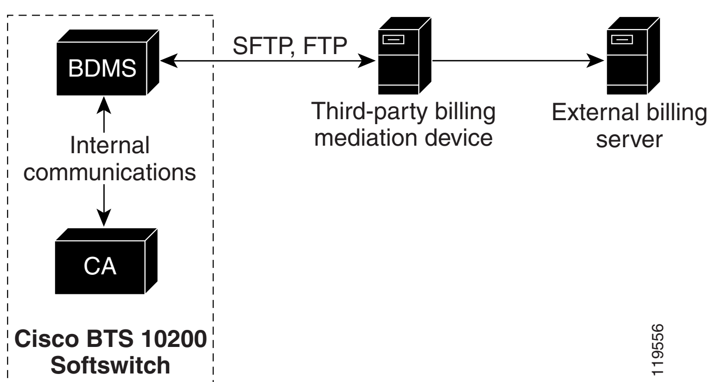
The BDMS provides the following billing functions:

- Supports batch record transmission via FTP and SFTP.
- Issues events as appropriate including potential billing data overwrites.
- Saves billing data records in persistent store—The allocated storage space is provisionable using CLI commands and can range from 10 MB to 5 GB (default 1 GB).
- Supports user-provisionable billing subsystem parameters.
- Supports on-demand CDB queries based on file name, time interval, call type, service type, termination cause, terminating number, originating number, or last record(s) written.

See the *Cisco BTS 10200 Softswitch Billing Interface Guide* for CDB billing procedures and for detailed descriptions of basic call billing data and feature billing data.

Note FTP sessions are used for file transfers initiated by the Cisco BTS 10200 Softswitch.

Figure 1-5 Billing Interface to the BDMS



MBA Functions

SIP phones interface via the IP network with the Mini-Browser Adapter (MBA) for services. The user accesses service functions via the "services" key on the SIP phone. A GUI on the SIP phone allows users to self-provision certain features. The MBA supports these services and performs GUI management for the GUI-enabled SIP-phone handsets.

Figure 1-2 shows the MBA and its interfaces:

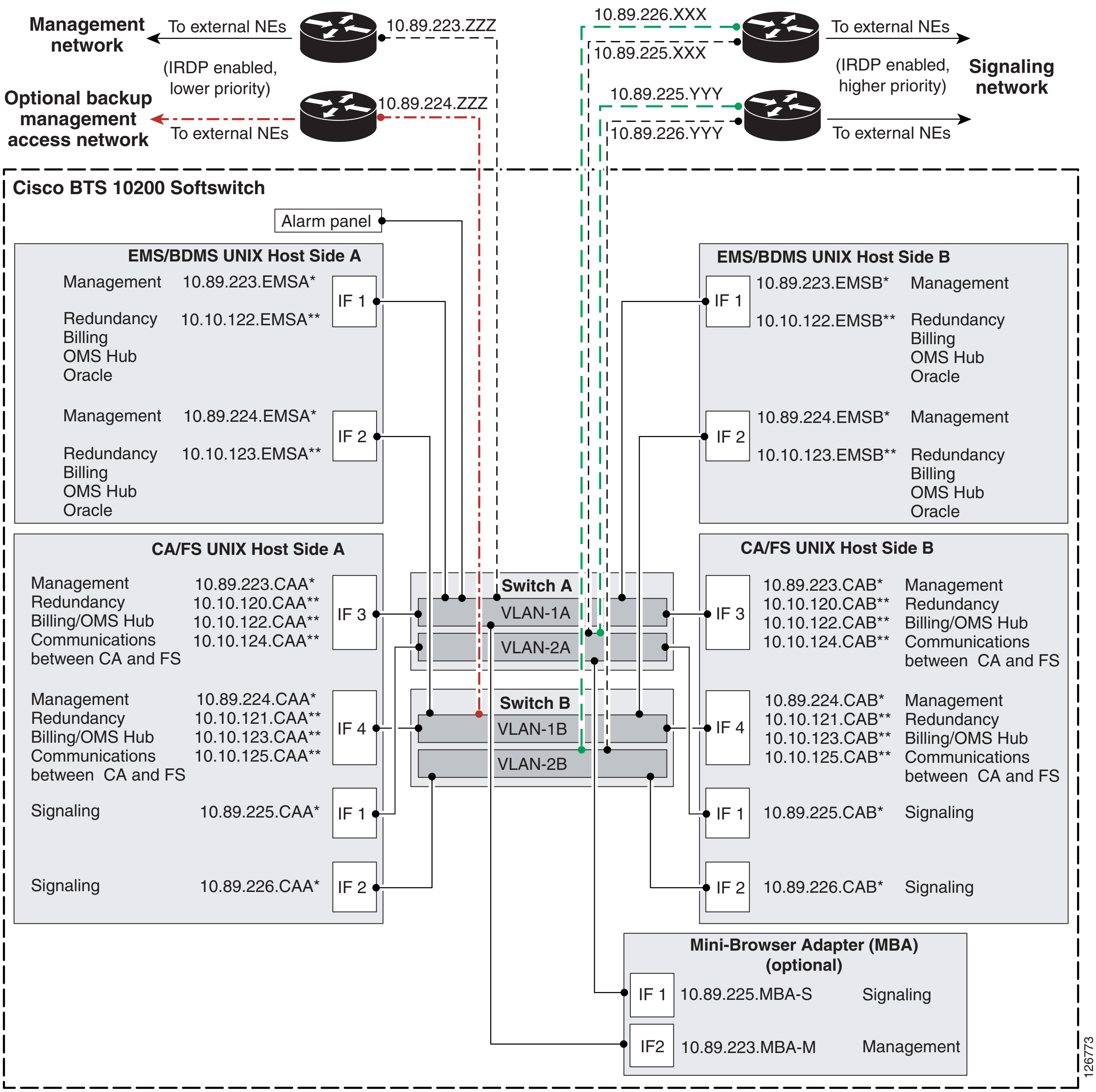
- The MBA interfaces with the GUI feature server (GFS) in the FSPTC. The GFS is the feature server data access component for GUI management, and is responsible for subscriber data access and northbound updates into the EMS. Internal signaling between the MBA and the GFS is via GUI Control Protocol (GCP), which is an XML-based protocol over SCTP links.
- Signaling between the MBA and SIP phones uses Cisco CMXML protocol over HTTP.

Reliability and Availability of Components

The Cisco BTS 10200 Softswitch network configuration is shown in Figure 1-6. This configuration provides redundant host machines for the EMS/BDMS and CA/FS components, redundant management local area networks (LANs), and six interfaces to the external routers. The configuration enhances security by separating management traffic from signaling traffic. As shown in the drawing, the service provider has the option of installing a backup management access network.

Note The MBA runs on a separate host machine and uses single (nonredundant) links for management and signaling.

Figure 1-6 Cisco BTS 10200 Softswitch Network Configuration



Notes for Figure 1-6:

1. The following labels represent specific components and functions:
   - IF = Interface.
   - A* and B* represent physical IP addresses; A** and B** represent logical IP addresses.

- Signaling: MGCP, SIP, and H.323 signaling functions use logical IP addresses that are migrated to the other signaling interface when the platform switches over.
- OMS Hub carries internal communications.

2. The IP addresses shown in the figure are for illustration purposes only. IP address examples beginning with 10.89 indicate externally viewable addresses, and those beginning with 10.10 indicate internal nonroutable addresses. The actual IP address data for each Cisco BTS 10200 Softswitch is in the *Network Information Data Sheet* that was supplied with your specific system.
3. ICMP Router Discovery Protocol (IRDP) advertisement must be enabled on the routers. IRDP on the management network routers must be set to a lower priority than the IRDP level on the signaling network.
4. "To external NEs" refers to the following links in the service provider network:
   - Uplinks for external access to hosts, used for management services (via SSH, SFTP, and so forth), DNS services, and outbound billing data (via FTP or SFTP).
   - Uplinks for external communications, used for connection to external NEs via an IRDP-enabled network.
5. The following restrictions apply for administrative access to the Cisco BTS 10200 Softswitch via the management network:
   - To access the management network of the Cisco BTS 10200 Softswitch from an external host, the external host must be in the same network as the management network.
   - If the external host is in a different network, the operator can set up a static route to each of the CA hosts, and this will allow the external host to access the management network.
6. To support full system redundancy, you must connect the external uplinks from the Catalyst switches to separate routers as shown in Figure 1-6:
   - There must be dual (redundant) signaling uplinks from each Catalyst switch, so that each Catalyst switch is connected to each signaling router.
   - There must be a single management uplink from Catalyst Switch A to one of the management routers. A second management uplink, from Catalyst B to the other management router, is optional.
   - The routers must be connected to separate networks with diverse routing paths to the applicable external NEs and services (such as OSS, DNS, media gateways, and announcement servers).

Caution If each external signaling uplink is not connected as described in Note #6., a single point of failure could cause a traffic interruption.

7. It is important to ensure redundancy of the DNS lookup function, so that this function is not completely lost in the event of a network outage. Cisco recommends that two (redundant) DNS units be deployed in the service provider network, and that the two DNS units be reachable via separate networks with diverse routing paths. Cisco recommends that you place the DNSs behind a load balancer so that a single IP address is exported to clients such as the Cisco BTS 10200 Softswitch.

Caution If both DNS servers become unreachable, a traffic interruption may occur.

8. The alarm panel refers to a terminal server (which could be a terminal server built into an alarm panel). It could be customer supplied or Cisco supplied, depending on the hardware options selected. The alarm panel supplied with some Cisco BTS 10200 Softswitch systems is not used for alarms or

for aggregation or reporting of machine alarms, but rather is used as a form of terminal concentrator. The Cisco BTS 10200 Softswitch software does not transmit machine alarms through this port. Instead, machine alarms are sent via alarm reports, as described in the *Cisco BTS 10200 Softswitch Operations, Maintenance, and Troubleshooting Guide*.

Dual Active/Standby Configuration

> **Note** This section is applicable to the EMS, BDMS, CA, and FS components, but not the MBA component. The MBA is not deployed in a dual configuration.

Each logical component (EMS, BDMS, CA, and FS) is deployed in a dual active/standby configuration, with the two sides running on separate computers (hosts). The active side of each component is backed up by a standby side on the other host. The communication paths among the components are also redundant. The redundant architecture supports the reliability and availability of the entire system. The active and standby sides of each logical component pair operate as follows:

- There is no traffic load sharing between the active and standby sides; the active side performs all of the call processing, and the standby does none.
- Call and feature data from the active side are replicated to the standby side at specific checkpoints of a call (when a call is answered, released, and so forth).
- An automatic internal audit function runs on the standby side of each component—EMS, BDMS, CA, and FS. It checks all the shared memory tables in the components to verify consistency and to check for any corruption. The audit reports any data structure inconsistencies or corruption via alarms and trace messages.
- Each side maintains a keepalive channel with the corresponding mate side. The keepalive process on each side determines if the mate is faulty. If there is a failure on the active side (or if the operator intentionally brings down the active side), the other side becomes active and takes over the traffic load. All stable calls continue to be processed without any loss of calls. There is no service outage, but during a switchover, transient calls can be impacted.

  > **Note** H.323 call stability relies on H.323 Annex E functionality at both H.323 endpoints.

  When the side that failed is brought back in service, it remains in standby mode and the system runs in normal duplex mode.
- IP Manager, a built-in IP management function, provides logical interfaces to several signaling-protocol components (such as MGCP, H.323, SIP) for remote devices on the currently active CA/FS. If IP Manager detects a CA/FS platform failover (from primary to secondary or vice-versa), it migrates the IP addresses of the logical interfaces over to the newly active CA/FS side.

  > **Note** IP Manager only migrates IP addresses on the same subnet. In the case of a multi-homed platform, when one of the interfaces fails, IP Manager does not migrate the IP address to a different interface.

- The operator can manually switch (force) either side to become active, which automatically forces the other side into standby mode.

Process Restartability

When a Cisco BTS 10200 Softswitch process exits due to an internal error (such as SIGSEGV on UNIX) or is terminated by the platform, the system automatically restarts the process that shut down. Restarting the process is a preferred alternative to switching over to the mate, because the restart preserves stable calls and also attempts to preserve transient calls. When a process is restarted, the process audits information such as resource states and attempts to repair inconsistencies. If a process experiences a high failure rate (even after repeated restarts), the system will switch over to the mate.

Cisco Specified Hardware

Note The MBA runs on a separate Sun host machine that is not part of the standard Cisco specified hardware set. Contact your Cisco account representative if you need additional information about the MBA component.

The Cisco BTS 10200 Softswitch software must be loaded on the appropriate Cisco specified hardware. These hardware options are listed in the *Cisco BTS 10200 Softswitch Release Notes*.

General Description and Important Notices

Each newly installed system requires the following devices:

- Four UNIX-based host machines running the Solaris operating system (see the *Cisco BTS 10200 Softswitch Release Notes* for applicable updates regarding Solaris patch levels)
- Two Cisco Catalyst 2950M XL Fast Ethernet Switches
- Terminal server (or alarm panel that includes a terminal server)
- DC power distribution unit (PDU) or two AC power strips, as applicable

Two host machines are used for the EMS/BDMS components and two host machines are used for the CA/FS components. The use of duplex host machines supports the redundancy operations of the logical components.

Equipment must be mounted in racks or cabinets that meet local service provider site requirements. Rack configurations can vary according to service providers requirements and preferences.

Note Consult your Cisco account team to determine which platform option best fits your current and future network requirements and traffic levels. Your Cisco account team can also provide you with options for purchasing hardware directly from Cisco or via reference sale.

Note Cisco TAC does not support hardware when purchased directly from Sun or another vendor. Hardware support contracts should be purchased from Sun, or a Sun Value Added Reseller.

Caution Be sure to use one of the hardware sets specified by Cisco in the in the *Cisco BTS 10200 Softswitch Release Notes*. Cisco TAC only supports Cisco BTS 10200 Softswitch systems running on these Cisco specified hardware configurations. The software is not supported on any other types or combinations of hardware.

Note See the "Site Preparation" section on page 1-22 for the site requirements applicable to these hardware sets. These requirements are essential to proper system operation.

Regulatory Compliance

The Cisco BTS 10200 Softswitch complies with the standards listed in Table 1-1.

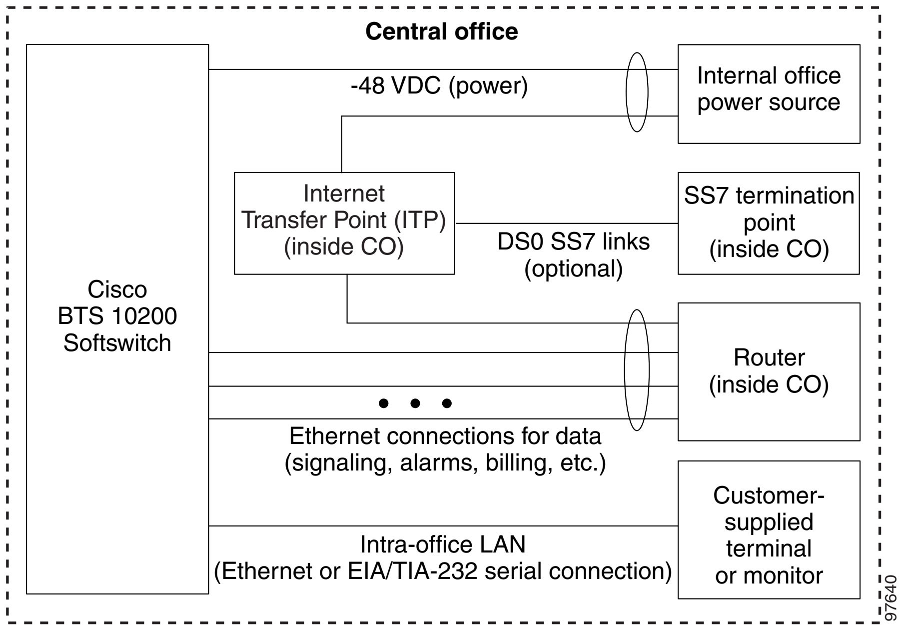
Table 1-1 Standards Compliance

Specification	Industry Standard
Information Technology Equipment	UL[1] 1950
EMI[2]	FCC[3] Class A (47CFR, Part 15)
Environmental compatibility	NEBS[4] Level 1 and Level 3 Requirements (SR-3580)

1. UL = Underwriters Laboratories
2. EMI = electromagnetic interference
3. FCC = Federal Communications Commission
4. NEBS = Network Equipment-Building System

The Code of Federal Regulations Title 47 (CFR 47) Part 68, *Connection of terminal equipment to the telephone network*, does not apply to this product. All of the points of demarcation are located at the first physical connection external to the Cisco BTS 10200 Softswitch frame, which are at customer-provided equipment internal to the central office (CO). See Figure 1-7 for a block diagram.

Figure 1-7 Cisco BTS 10200 Softswitch Connection to Internal CO Equipment



Site Preparation

This section describes the installation site requirements for the Cisco BTS 10200 Softswitch. Installation procedures are provided separately.

Required Facilities

The Cisco BTS 10200 Softswitch interfaces with a variety of NEs using various protocols. The facilities connecting the Cisco BTS 10200 Softswitch to these NEs are customer supplied.

Intershelf Cables

The procedures for cabling the intershelf cables (those that connect the various host machines and Ethernet Switches within the Cisco BTS 10200 Softswitch) are documented in the *Cisco BTS 10200 Softswitch Cabling and IRDP Procedures*. If your hardware was purchased as part of a complete integrated and tested system from Cisco Systems, the intershelf cables are included with your order.

Cables for Connection to External NEs

Cables for connections to external NEs are not included with the Cisco BTS 10200 Softswitch order, and are customer supplied.

Operator Access to the Cisco BTS 10200 Softswitch

System administrators and operators can access the Cisco BTS 10200 Softswitch via a number of interfaces, including secure shell (SSH) session to the EMS over Ethernet, and via OSS and NMS connections. Communications can be interactive or via batch mode (batch mode uses SFTP). See the "EMS Functions" section on page 1-11 for additional user interface options.

Site Environmental and Power Requirements

The environmental and power requirements for installation of the Cisco BTS 10200 Softswitch are documented in the *Cisco BTS 10200 Softswitch Building Environment and Power Site Survey* document, available from your Cisco account team.

Caution Cisco strongly recommends that you use uninterruptible power for both AC and DC systems. The uninterruptible supply should be engineered to support system operation through any possible power interruption.

Caution For DC-powered installations, the power must come from two separate dedicated DC branches (redundant "A" and "B" feeds) for each DC-powered Cisco BTS 10200 Softswitch. For AC-powered installations, two separate (redundant) circuits are required. The AC circuits must be sourced from separate transformer phases on separate breakers such that a single breaker trip will not disable both.

Network Data Definition

Certain network data needs to be provided to Cisco so that each Cisco BTS 10200 Softswitch node can be given the appropriate initial software configuration. This configuration ensures that the Cisco BTS 10200 Softswitch will be able to communicate with the service provider network. Contact your Cisco account team to receive a *Network Site Survey* applicable to your specific system when preparing this information. Your Cisco account team will use the information you provide in the *Network Site Survey* to set up the initial software configuration for your system, and will provide you with a record of this data in a *Network Information Data Sheet*.

Network Communications Paths

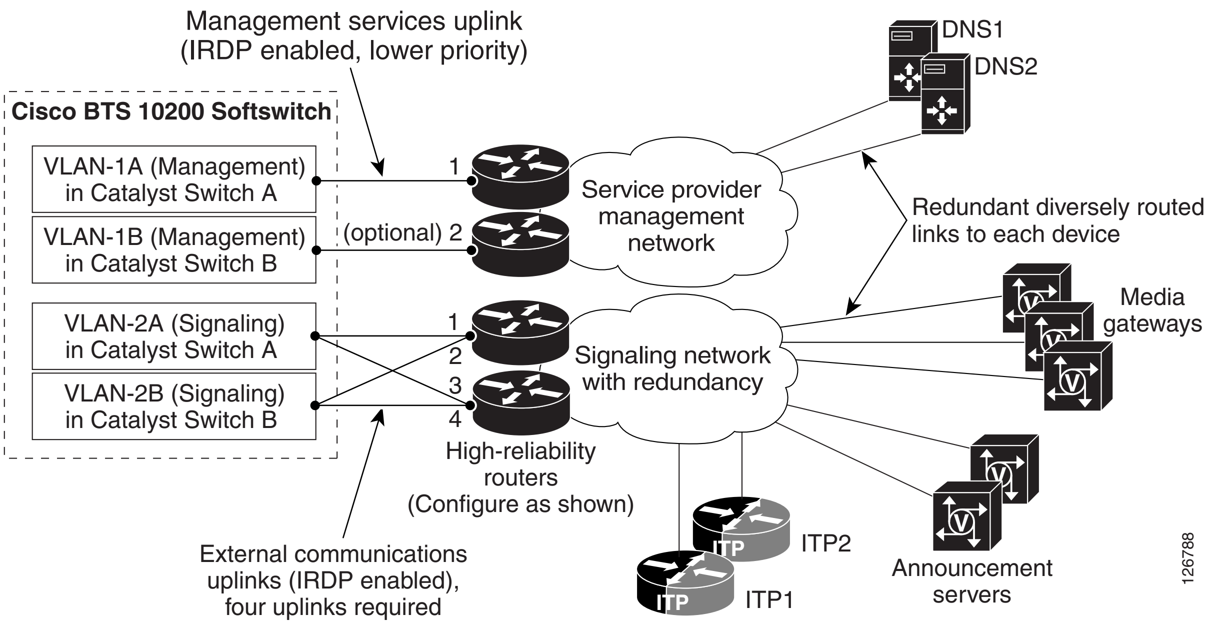
The Cisco BTS 10200 Softswitch relies on ICMP Router Discovery Protocol (IRDP) for dynamic updating of router tables. The routers used for external communication between the Cisco BTS 10200 Softswitch and the service provider network are assumed to be IRDP capable, and the service provider network is assumed to be IRDP capable. (If this is not the case, contact Cisco for a review of configuration options.) During installation, the service provider should turn on IRDP in these routers.

Note IRDP is an extension to Internet Control Message Protocol (ICMP) that provides a mechanism for routers to advertise useful default routes.

Figure 1-8 shows an example of communication paths between the Cisco BTS 10200 Softswitch and NEs in the managed network. The initial software configuration of the Cisco BTS 10200 Softswitch enables it to communicate with external NEs.

Caution To ensure proper functioning of the network, you must configure the network with at least the level of redundancy, diverse routing, and IRDP functionality shown in this drawing. Otherwise, a single point of failure could cause a traffic interruption.

Figure 1-8 Uplinks and Communications Paths to NEs in the Managed Network



Notes for Figure 1-8:

1. IRDP on the management network routers must be set at a lower priority that the IRDP level on the signaling network.
2. The uplinks are used as follows:
   a. Two uplinks for management services (via connection modes such as SSH and SFTP), DNS services, and outbound billing (via FTP and SFTP).
   b. Four uplinks for external communications for VoIP signaling based on protocols such as MGCP, SIP, H.323, COPS, SIGTRAN, and so forth.

   Note The four signaling uplinks must be connected to the appropriate internal VLANs of the Cisco BTS 10200 Softswitch as shown in Figure 1-8.

3. To support full system redundancy, you must connect the six external uplinks to four separate routers as shown in Figure 1-8. Furthermore, you must also connect the routers to separate networks with diverse routing paths to the applicable external NEs and services (such as DNSs, ITPs, media gateways, and announcement servers).

Caution If each of the external uplinks is not connected as described in Note #3., a single point of failure could cause a traffic interruption.

4. The Cisco BTS 10200 Softswitch does not store or use absolute IP addresses. Instead, it locates network connections by looking up domain names on the service provider domain name server (DNS). The service provider DNS translates the domain names into IP addresses. During software installation, the Cisco BTS 10200 Softswitch is configured with the data it needs to communicate with the service provider DNS. This configuration data is stored in the opticall.cfg file, and some critical domain names are also populated in the etc/hosts file in each host machine. To ensure redundancy of the DNS lookup function in the event of a network outage, Cisco recommends that two (redundant) DNS units be deployed in the service provider network, and that the two DNSs be reachable via separate networks with diverse routing paths. Cisco recommends that you place the DNSs behind a load balancer so that a single IP address is exported to clients such as the Cisco BTS 10200 Softswitch.

Caution If both DNS servers become unreachable, a traffic interruption may occur.

CHAPTER 2

Supported Signaling Protocols

Revised: March 19, 2007, OL-5906-14

The Cisco BTS 10200 Softswitch supports the following types of external signaling protocols:

- MGCP line
- MGCP CAS
- SIGTRAN (for SS7 applications), including North America, China, and Mexico ISUP support
- ISDN (PRI)
- H.323
- SIP and SIP-T
- PacketCable-based signaling protocols:
  - Network-Based Call Signaling (NCS) protocol
  - Trunking Gateway Control Protocol (TGCP)
  - DQoS/COPS query and response protocol
  - RADIUS authentication protocol (IETF RFC 2865)

These signaling types are described in more detail in the sections that follow:

- MGCP Line Signaling Support
- MGCP CAS Signaling Support
- SS7 Signaling Support via SIGTRAN
- ISDN Signaling Support
- H.323 Signaling Support
- SIP and SIP-T Signaling Support
- PacketCable-Based Signaling Support

Note For lawful intercept and CALEA information, see the "Lawful Intercept Interface" section on page 3-17.

MGCP Line Signaling Support

Media gateways (MGWs) provide bearer paths between voice and packet networks. MGWs also provide connection control, endpoint control, auditing, and status functions. These gateways are equipped with voice coders that convert voice into packets, and voice decoders that convert packets into voice. Connections are grouped in calls, which means that a call can have one or more connections. One or more Call Agents (CAs) sets up the connections and calls.

The Cisco BTS 10200 Softswitch connects to a variety of MGWs using Media Gateway Control Protocol (MGCP), and provides voice over IP (VoIP) bearer path control. This implementation is based upon the evolving industry standards for MGCP, including the following MGCP variants:

- MGCP (IETF Version 0.1, Draft 5, February 1999)
- MGCP (IETF RFC 2705, Version 1.0, October 1999)

Note The MGCP-VERSION and MGCP-VARIANT parameters in the MGW-PROFILE table are used to identify the MGCP version and variant that an MGW supports.

General Functions of MGCP Interface

The MGCP interface performs the following functions:

- Handles MGW initialization
- Provides endpoint auditing
- Provides MGW fault management
- Provides maintenance and administration of each termination, MGW operational states, and so forth
- Carries call-control signaling
- Carries media-path control signaling

Special Functions of MGCP Interface

The Cisco BTS 10200 Softswitch supports several special-purpose MGCP-based functions:

- Codec selection service—The process a CA uses to find a common codec (coder/decoder) type between an originating and terminating call leg so a call can go through. The preferred codec type for originating and terminating calls is provisioned by the service provider using the QoS table in the Cisco BTS 10200 Softswitch database. The QoS can be configured for a subscriber or trunk group (TG). The CA makes a decision on actual codec type based on a combination of the following conditions:
  - Codec types available on the MGW—The MGW dynamic profile (list of supported codecs reported by MGW) or MGW static codec list (list of supported codecs configured in the Cisco BTS 10200 Softswitch).
  - The codec type provisioned in the QoS table—If a certain codec type is provisioned in the QoS table but not available in the MGW dynamic profile or TG profile, that type cannot be used. When no matching code is found, default pulse code modulation mu-law (PCMU) codec is used.

  The following codec types are supported:
  - G.711 mu-law (PCMU)—Default value for codec type

- G.711 A-law (PCMA)
- G.723.1 High rate
- G.723.1 Annex A High rate
- G.723.1 Low rate
- G.723.1 Annex A Low rate
- G.729
- G.729 Annex B
- G.726 32K rate
- G.726 24K rate
- G.726 16K rate
- G.728

- Resource Reservation Protocol (RSVP)—An Internet Engineering Task Force (IETF) protocol for providing integrated services and reserving resources on the IP network. The service provider provisions the preferred reservation profile (guaranteed, controlled load, or best effort) in the QoS table. When a reservation is needed on a connection, the Cisco BTS 10200 Softswitch specifies the preferred reservation profile to the gateway. Whether or not RSVP will be done depends on the configuration of the gateway as well as the preferred reservation profile specified by the Cisco BTS 10200 Softswitch. If the best effort RSVP profile is specified, RSVP is not performed.
- Announcement server—A media server that stores network-based announcements and plays them to a caller upon request from the Cisco BTS 10200 Softswitch. The announcement server interfaces with the Cisco BTS 10200 Softswitch using MGCP. Every Cisco BTS 10200 Softswitch in the network requires its own announcement server.
- Dual tone multifrequency (DTMF) signaling—Signaling that is transported across the IP network under MGCP control.
- Channel-associated signaling (CAS)—Signaling that is used with the MGCP interworking function.
- Voice over ATM (VoATM) support—Configurable parameters that support ATM extensions (AAL1, AAL2, and AAL5) on MGCP.

Note The ATM adaptation layer (AAL) is a standards layer that allows multiple applications to have data converted to and from an ATM cell. It uses a protocol that translates higher layer services into the size and format of an ATM cell.

MGCP CAS Signaling Support

The Cisco BTS 10200 Softswitch supports the following MGCP CAS interfaces:

- Public safety answering point (PSAP) systems interface for 911 emergency services
- Operator services interface, including legacy operator services interface via MF/T1 trunks
- PBX interfaces

Note CAS is used with the MGCP interworking function.

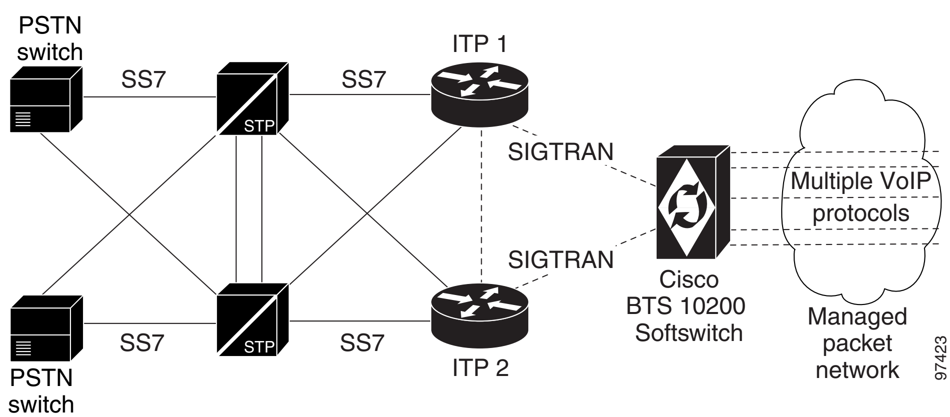
SS7 Signaling Support via SIGTRAN

The Cisco BTS 10200 Softswitch communicates with Signaling System 7 (SS7)-based PSTN switches and service control points (SCPs) by using a SIGTRAN-based signaling gateway (SG). The SIGTRAN interface carries all SS7 messages encapsulated in IP packets. The Cisco IP Transfer Point (ITP) is one of the SGs used with the Cisco BTS 10200 Softswitch for this purpose.

Interface to the SS7 Network

The basic interface of the Cisco BTS 10200 Softswitch to the SS7 network is shown in Figure 2-1.

Figure 2-1 Cisco BTS 10200 Softswitch Interface to SS7 Network



Note For information on compatibility with specific Cisco ITPs, see the "Cisco ITP Signaling Gateways" section in the *Cisco BTS 10200 Softswitch Release Notes*.

The Cisco BTS 10200 Softswitch can be configured to have multiple originating point codes (OPCs). For information on OPCs and subsystems, see the "Originating Point Codes" section in the *Cisco BTS 10200 Softswitch Release Notes*.

For additional information, see the following standards and industry documents:

- ANSI T1.113, *Telecommunications Signaling System No. 7 (SS7) - Integrated Services Digital Network (ISDN) User Part (ISUP)*
- GR-317-CORE, *Switching System Requirements for Call Control Using the Integrated Services Digital Network User Part*
- GR-394-CORE, *Switching System Generic Requirements for Interexchange Carrier Interconnection using the Integrated Services Digital Network User Part*
- GR-533-CORE, *LSSGR: Database Services Service Switching Points - Toll-Free Service*
- GR-1188-CORE, *LSSGR: CLASS Feature: Calling Name Delivery Generic Requirements*
- IETF RFC 2960, *Stream Control Transport Protocol (SCTP)*
- IETF draft-ietf-sigtran-sua-14.txt, *Signalling Connection Control Part User Adaptation Layer (SUA)*

Support for ISUP Variants

The Cisco BTS 10200 Softswitch supports the following ISUP variants:

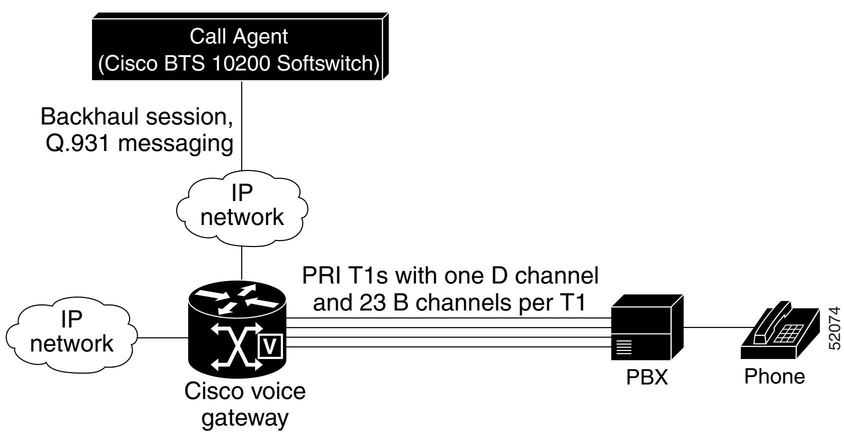
- ITU93 White Book ISUP—Release 4.1 and later
- European Telecommunications Standards Institute (ETSI) v2 ISUP—Release 4.4.1 and later
- ANSI ISUP (for NANP region)—Release 3.5 and later
- China—Release 4.1 and later
- Mexico—Release 4.1 and later

ISDN Signaling Support

This section describes the Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) variants and supplementary services supported by the Cisco BTS 10200 Softswitch. ISDN PRI allows the Cisco BTS 10200 Softswitch to interconnect to small and medium businesses using legacy PBX PRI interfaces. The basic ISDN network elements and signaling connections are shown in Figure 2-2.

Note Standby elements in the figure are omitted for clarity.

Figure 2-2 Example of ISDN Network Elements



The design provides for transport of PRI information elements (IEs) and messages. Interoperability is supported with the following PRI variants:

- Nortel DMS-100
- AT&T 4ESS
- Lucent 5ESS
- NI2

The Cisco BTS 10200 Softswitch supports the following capabilities:

- ISDN T1 PRI
- Q.921 and Q.931 network side
- ISDN backhaul communication of Q.931 messages from MGWs to the Cisco BTS 10200 Softswitch

- Support for Facility Associated Signaling (FAS)
- Support for Non-Facility Associated Signaling (NFAS) (Release 4.4.1 only)
- Support for Backup D channel (Release 4.4.1 only)

Note For additional details and procedures for the Cisco BTS 10200 Softswitch ISDN implementation, see the *Cisco BTS 10200 Softswitch ISDN Provisioning and Troubleshooting Guide*.

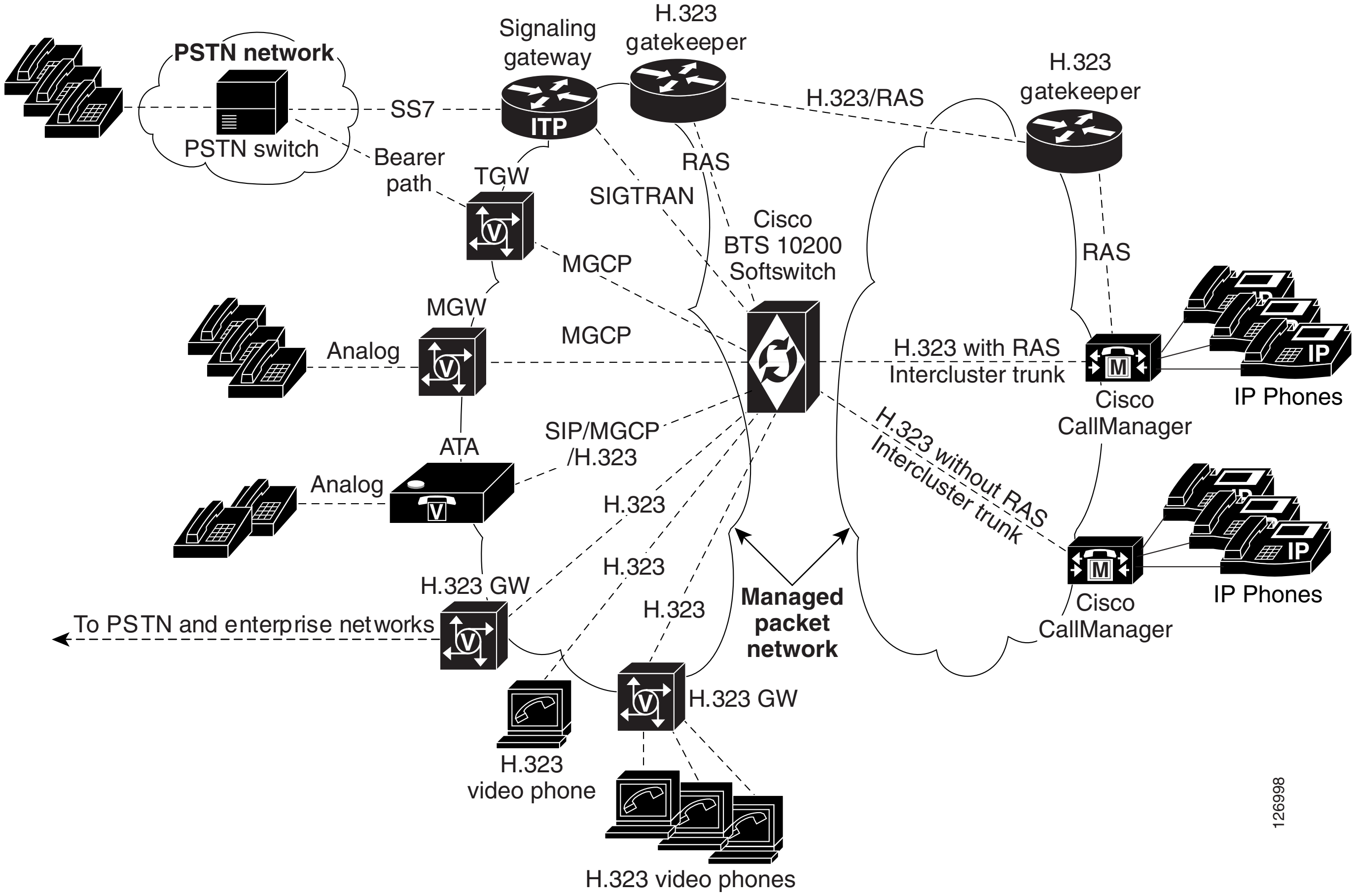
H.323 Signaling Support

The Cisco BTS 10200 Softswitch functions as a logical H.323 gateway to communicate with H.323 gatekeepers (GKs), and with Cisco CallManager and other H.323 gateways. The Cisco BTS 10200 Softswitch also provides signaling for other trunks and lines over MGCP and SIP protocols. In addition, it communicates with signaling gateways (SGs) for SS7 signaling and with trunking gateways (TGWs) that provide the bearer path to the PSTN. This allows H.323 Internet VoIP traffic to be carried seamlessly into the PSTN networks.

These signaling links are shown in Figure 2-3.

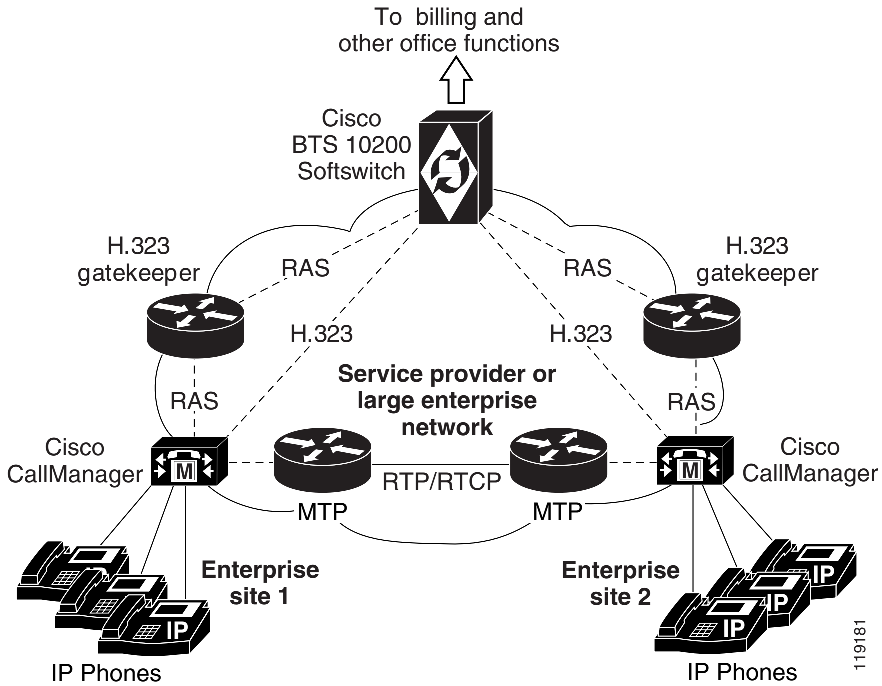
Note The Cisco BTS 10200 Softswitch can be configured as up to four logical H.323 gateways.

Figure 2-3 Signaling Links between Cisco BTS 10200 Softswitch, Cisco CallManager, and Other Service Provider NEs



The interoperability between the Cisco BTS 10200 Softswitch, Cisco CallManager, and Cisco IOS H.323 gateways enhances the delivery of call control features between enterprise networks and service provider networks. These systems interoperate to provide subscriber features such as call forwarding, call waiting, call transfer, and three-way calling. The Cisco BTS 10200 Softswitch can be used to connect calls between two phones that reside on different Cisco CallManager systems (see Figure 2-4). Signaling of certain information, for example connected name and number information, is transparently passed from the terminating Cisco CallManager via the Cisco BTS 10200 Softswitch back to the originating Cisco CallManager.

Figure 2-4 Example of Connecting Calls from Phones on Separate Cisco CallManager Systems



Note For additional technical discussion, prerequisites, and provisioning steps, see the *Cisco BTS 10200 Softswitch H.323 Protocol Guide*.

SIP and SIP-T Signaling Support

The Cisco BTS 10200 Softswitch uses Session Initiation Protocol (SIP) and SIP for telephones (SIP-T) signaling to communicate with other SIP-based network elements. This implementation is based upon the evolving industry standards for SIP, including IETF document *RFC 3261, SIP: Session Initiation Protocol*.

Note This section provides an overview of SIP implementation on the Cisco BTS 10200 Softswitch. For SIP feature details and applicable procedures, see the *Cisco BTS 10200 Softswitch SIP Protocol Guide* and the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

SIP Functions

The Cisco BTS 10200 Softswitch supports both SIP trunks and SIP-based subscriber lines (SIP phones). It provides the following SIP-related functions:

- Protocol conversion between SIP and several other protocols, including SS7, PRI, H.323, MGCP, and CAS.
- Tandem back-to-back user agent (UA) for direct SIP-to-SIP calls (trunk to trunk, phone to phone, and trunk to/from phone), and SIP-to-SIP-T calls.

> **Note** There is no provisioning associated with the back-to-back UA functionality. The Cisco BTS 10200 Softswitch automatically acts as a back-to-back UA when there is a SIP-to-SIP call.

- SS7 bridging between softswitches using SIP-T methods.
- Native support of SIP endpoints such as SIP phones, including authentication and registration management. (For example, the Cisco BTS 10200 Softswitch maintains the current location of SIP subscribers.)

SIP roles performed by the Cisco BTS 10200 Softswitch include:

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

Applicable SIP references are listed in the "SIP and SIP-T References" section on page 2-10.

SIP Features

The Cisco BTS 10200 Softswitch supports the following SIP features:

- Reliable provisional response
- 3XX redirect response on SIP trunks
- SIP hairpin
- Third-party call control (3PCC)
- ANI-based routing for SIP calls
- DTMF relay for communications with interactive voice response (IVR) servers
  - SUBSCRIBE/NOTIFY method
  - INFO method
- Message waiting indicator
- Diversion header
- UAC and UAS forking
- SIP session timer
- Type of service (ToS) for SIP signaling
- DNS services (DNS SRV) lookup for initiating SIP calls
- DNS naming authority pointer (NAPTR) lookup for initiating SIP calls
- Mapping the carrier identification code (CIC) in the SIP uniform resource identifier (URI) to a transit network selection (TNS)
- SIP Register
- SIP Authentication
- SIP Refer
- SIP trunk audit
- SIP-trunk route advance with provisionable timer for Invite retransmission

SIP-T Support

The Cisco BTS 10200 Softswitch supports SIP-T functions. SIP-T is used to bridge calls between two SS7 networks. SIP-T encapsulates the SS7 ISUP information elements (based on GR-317 ISUP version) and carries them through the packet network. It provides for encapsulation/decapsulation at the PSTN gateways and helps route the call through the packet network. SIP-T functionality is described in *IETF RFC 3398, Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping*.

FCP Interface

The Cisco BTS 10200 Softswitch uses Feature Control Protocol (FCP) for internal communications between the Call Agent (CA) and Feature Server (FS) components. FCP is a Multipurpose Internet Mail Extension (MIME) application on top of SIP. FCP uses SIP for transport, and carries call state control and status information needed for feature control.

SIP Billing Support

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

SIP and SIP-T References

The following IETF documents are applicable to SIP and SIP-T functionality. In addition, a number of IETF draft documents are applicable. For a complete list of references, see the *Cisco BTS 10200 Softswitch SIP Protocol Guide*.

- RFC 2617, *HTTP Authentication*
- RFC 3261, *SIP: Session Initiation Protocol*
- RFC 3262, *Reliability of Provisional Responses in the Session Initiation Protocol (SIP)*
- RFC 3263, *Session Initiation Protocol (SIP): Locating SIP Servers*
- RFC 3265, *Session Initiation Protocol (SIP)-Specific Event Notification*
- RFC 3311, *The Session Initiation Protocol (SIP) UPDATE Method*
- RFC 3398, *Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping*
- RFC 3372, *Session Initiation Protocol for Telephones (SIP-T): Context and Architectures*
- *RFC 2976, SIP INFO method*

PacketCable-Based Signaling Support

In a PacketCable-based network, the Cisco BTS 10200 Softswitch functions as both a call management server (CMS) and a media gateway controller (MGC).

PacketCable-Based Functions

The Cisco BTS 10200 Softswitch provides call control, call routing, and signaling for several types of network elements:

- Multimedia terminal adapters (MTAs) and embedded MTAs (EMTAs)
- Cable modem termination systems (CMTSs)
- Trunking gateways (TGWs)

The Cisco BTS 10200 Softswitch supports cable access for voice application, including communications with the Cisco UBR 7246 and Cisco UBR 924 universal broadband routers. It also provides interfaces to Record Keeping Servers (RKSs) for billing purposes, and IP security functionality.

The Cisco BTS 10200 Softswitch provides support for the following PacketCable-based protocols and functions:

- Network-Based Call Signaling (NCS) protocol.
- Trunking Gateway Control Protocol (TGCP).

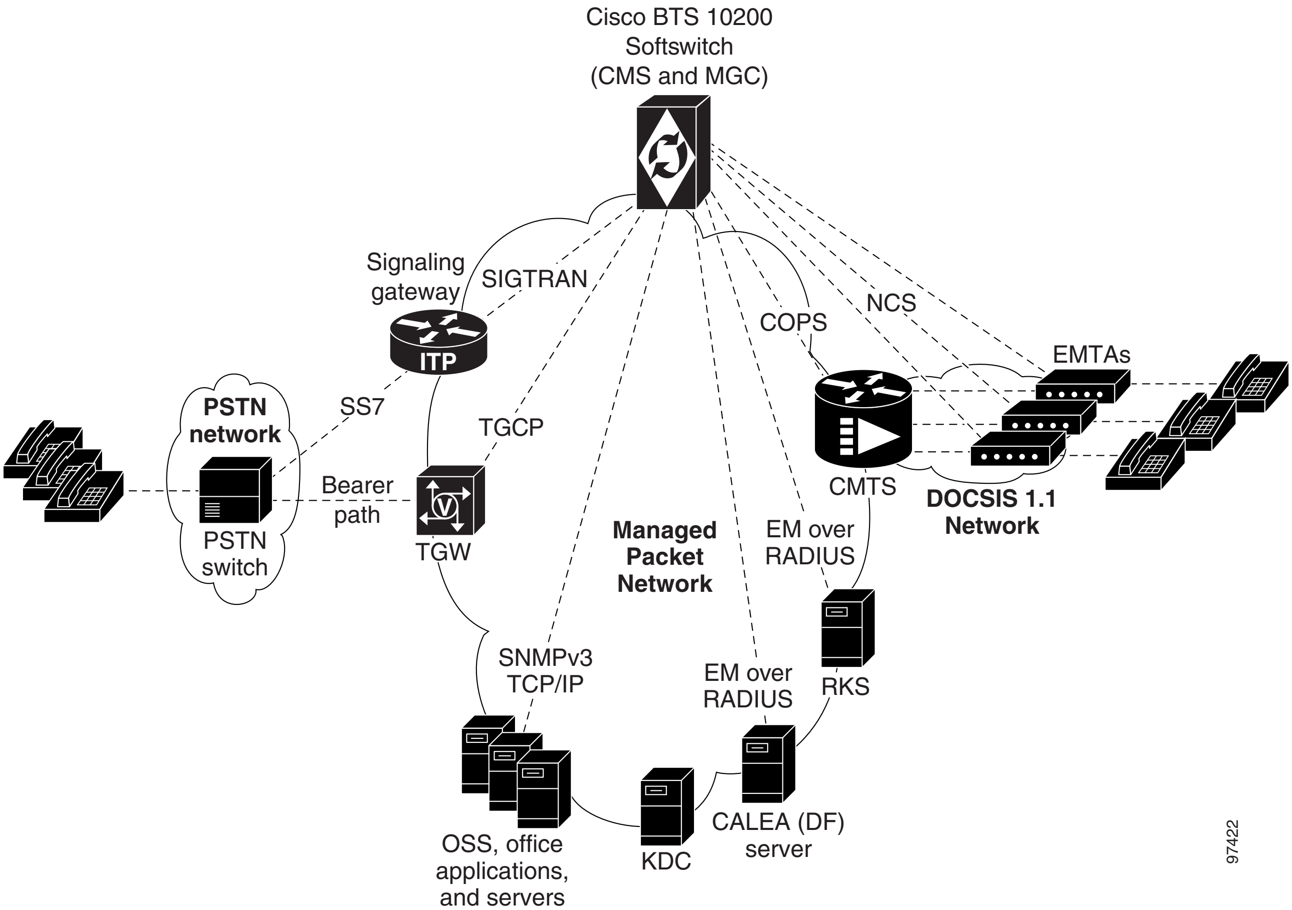
Note NCS protocol and TGCP are based on MGCP; they are referred to as profiles of MGCP.

- Dynamic Quality of Service (DQoS)/Common Open Policy Service (COPS) query and response protocol.
- RADIUS authentication protocol (IETF RFC 2865), used for transmission of event messages (EMs) to an external RKS for billing purposes.
- Security features, including implementation of IP security architecture (IPsec), and key management using Internet Key Exchange (IKE) and Kerberos.
- Interface for support of lawful intercept and the Communications Assistance for Law Enforcement Act (CALEA). See the "Lawful Intercept Interface" section on page 3-17 for a description of this feature.

Note For detailed information on compliance to specific paragraphs of the IETF standards (for TGCP, IP Security, NCS, and so forth), contact your Cisco account team.

Figure 2-5 shows a typical network with PacketCable-based network elements and the applicable external interfaces of the Cisco BTS 10200 Softswitch.

Figure 2-5 Example of PacketCable-Based Network Architecture



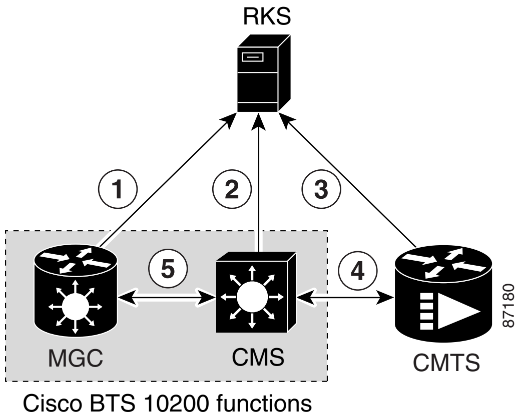
Event Message Implementation

This section describes the implementation of the event message (EM) feature on the Cisco BTS 10200 Softswitch. EMs are real-time call data records containing information about network usage and activities. They are typically used for billing purposes in a PacketCable-based network. The Cisco BTS 10200 Softswitch (which performs the CMS and MGC functions) transfers EMs to an external Record Keeping Server (RKS) that assembles call detail records (CDRs) from the EMs.

Note Event messages are also transmitted over RADIUS from the Cisco BTS 10200 Softswitch to a CALEA interface, with IPsec for encryption and authentication, and IKE for key management.

Figure 2-6 illustrates the PacketCable network elements and interfaces involved in the generation and processing of EMs.

Figure 2-6 Event Message Interfaces



Notes for Figure 2-6:

1. **MGC to RKS**—EMs generated by the MGC function in the Cisco BTS 10200 Softswitch are sent to the RKS.
2. **CMS to RKS**—EMs generated by the CMS function in the Cisco BTS 10200 Softswitch are sent to the RKS.
3. **CMTS to RKS**—EMs generated by the CMTS are sent to the RKS. The Cisco BTS 10200 Softswitch (MGC/CMS) is not involved.
4. **CMS to CMTS**—The CMS function in the Cisco BTS 10200 Softswitch sends the Billing Correlation ID (BCID) to the CMTS using the DQoS GateSet message.
5. **CMS to MGC**—There is an internal exchange of originating/terminating information such as BCID and FEID.

Note For additional technical discussion, prerequisites, and provisioning steps, see the *Cisco BTS 10200 Softswitch PacketCable Protocol Guide*.

Security Implementation

The implementation of PKT-SP-SEC-I07-021127, *PacketCable Security Specification*, November 27, 2002, provides a security scheme for the voice-over-cable network based on a set of security protocols. These protocols, based on the documents listed below, provide authentication (to help prevent theft of bandwidth, denial-of-service attack, replay, and so forth) and enable message integrity, privacy, and confidentiality.

- IETF documents covering IP security (IPsec) architecture:
  - RFC 2401, *Security Architecture for the Internet Protocol*, November 1998
  - RFC 2406, *IP Encapsulating Security Payload (ESP)*, November 1998
- IETF documents covering key management protocols IKE and Kerberos with extensions:
  - RFC 2409, *The Internet Key Exchange (IKE)*, November 1998
  - RFC 1510, *The Kerberos Network Authentication Service (V5)*, September 1993, with updates presented in PKT-SP-SEC-I06-021018

The Cisco BTS 10200 Softswitch performs the security functions of the CMS and MGC in the PacketCable environment. It supports security in accordance with PKT-SP-SEC-I07-021127 for both signaling and media:

- Signaling security—For signaling from CMS to eMTA, CMS to CMTS, and MGC to TGW
- Media (bearer) security—For signaling between originating eMTA and terminating eMTA, which is facilitated by the CMS during call signaling setup.

A special parameter, IPSEC_ENABLED, must be set in the opticall configuration file (opticall.cfg) at the time of software installation to enable the IPsec feature. The IPSEC_ENABLED value cannot be changed using CLI commands.

Note The value of the IPSEC_ENABLED parameter, and all other opticall.cfg parameters for your installation, is listed in the *Network Information Data Sheet* that Cisco provided with your system.

CHAPTER 3

Network Features

Revised: March 19, 2007, OL-5906-14

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

- Digit Manipulation
- Numbering Plans and Dialing Procedures
- Emergency Services (911)
- Operator Services
- Network Services

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

Note For information on subscriber features, see Chapter 4, "Subscriber Features." For information on outgoing call restriction options (Class of Service and Outgoing Call Barring) see Chapter 5, "Class of Service Restrictions and Outgoing Call Barring."

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 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 Cisco BTS 10200 Softswitch. (These values are listed in the Vertical Service Code appendix of the *Cisco BTS 10200 Softswitch Command Line Interface Reference 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, Maintenance, and Troubleshooting Guide*.

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 Cisco BTS 10200 Softswitch.

Note 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:

- Robust 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 Cisco BTS 10200 Softswitch performs digit manipulation by matching and replacing digits in the digit string that is being processed. For details on the rules used in this process, see the *Cisco BTS 10200 Softswitch Operations, Maintenance, and Troubleshooting Guide*.

Numbering Plans and Dialing Procedures

The Cisco BTS 10200 Softswitch supports the numbering plans and dialing procedures listed in Table 3-1. These features are described in the sections that follow.

Table 3-1 Support for Numbering Plans and Dialing Procedures

Feature Description	Reference
E.164 Dialing Plan Implementation	ITU-T Recommendation E.164
Casual Dialing (Dial Around)	
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, 611, 711, 811)	GR-532-CORE FSD-30-16-0000

E.164 Dialing Plan Implementation

The Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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)
- 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)

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

Tip [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 Cisco BTS 10200 Softswitch 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

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 3-2 lists several examples.

Table 3-2 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 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

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

The Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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 3-11 for a description.
- 900/976 information service calls—See the "Information Service Calls (900 and 976)" section on page 3-5 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, 611, 711, 811)

Note 911 service is covered in the "Emergency Services (911)" section on page 3-8.

This section describes Cisco BTS 10200 Softswitch support for n11 services. The typical relationship between the n11 codes and the nature of dial (NOD) values is as follows. The NOD values are listed in the *Cisco BTS 10200 Softswitch Command Line Reference Guide*.

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

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 Cisco BTS 10200 Softswitch 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 3-4.

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.

Other n11 Codes

The 511 code (caller access to information about local traffic conditions) is not supported in this release of the Cisco BTS 10200 Softswitch.

Emergency Services (911)

The Cisco BTS 10200 Softswitch 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*

Note 911 is typically used in the United States; other digit strings are used elsewhere in the world. 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.

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.

Note 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 Cisco BTS 10200 Softswitch 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.

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.

Note The emergency service (911) feature can be made available to all subscribers lines connected to a Cisco BTS 10200 Softswitch using the default office service ID. See the "Default Office Service ID" section on page 4-72 for a general description of this provisionable service.

Operator Services

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

- Subscriber Access to Operator, page 3-9
- Busy Line Verification (BLV) and Operator Interrupt (OI) Services, page 3-10

Subscriber Access to Operator

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. 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

Operator services provided to callers 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 Cisco BTS 10200 Softswitch using the default office service ID. See the "Default Office Service ID" section on page 4-72 for a general description of this provisionable service.

Feature Interactions

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

- The BLV feature does not support interaction with features currently invoked by the verified party (terminating subscriber) at the time of verification. If the verified party is engaged in a call and has any features invoked, the operator will receive a busy tone and will 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.
- 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.

Network Services

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

Table 3-3 Support for Network Services

Feature Description	Reference
8XX (Toll-Free Calling)	SR-2275, Sec. 14.6
Calling Party Number Options for Outgoing SETUP Messages	
Dialing Parity (IntraLATA Toll Presubscription)	FSD-20-24-0040 TR-TSY-000693
Lawful Intercept Interface	PKT-SP-EM-I08-040113
Local Number Portability (LNP)	ATIS/T1S1 T1.TRQ-02-2001
Network Loopback Test for NCS/MGCP Subscriber Endpoints	
Split-NPA	INC97-0404-016
T.38 Fax Relay	IETF RFC 2833 ITU-T *Recommendation T.38*
Trunk Testing	

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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch using the default office service ID, or to all subscribers in a specific POP using the office service ID. See the "Default Office Service ID" section on page 4-72 for a general description of this provisionable service.

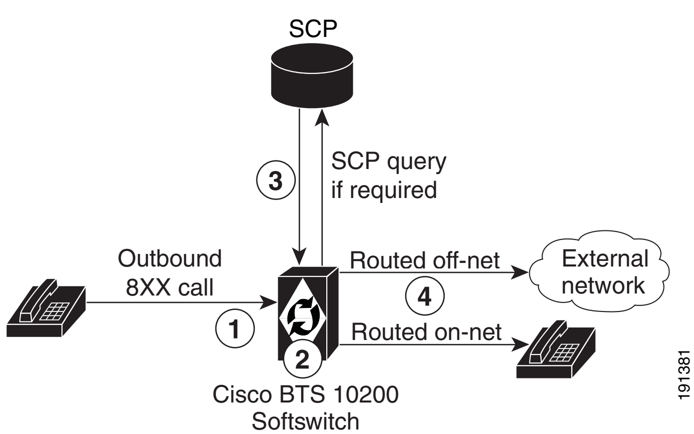
8XX Call Processing

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.
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.

Figure 3-1 shows the processing of an outbound 8XX call placed by a subscriber.

Figure 3-1 Processing of an Outbound 8XX Call



Notes for Figure 3-1

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).

Local Toll-Free Database

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

The Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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.*

Calling Party Number Options for Outgoing SETUP Messages

This feature allows the service provider to control the calling party number (CPN) data sent in the outbound SETUP message on redirected calls outbound from the Cisco BTS 10200 Softswitch 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
- Redirection of a basic or Tandem call

Figure 3-2 shows an example of the networks and phones involved in redirection by a subscriber phone. Table 3-4 explains how to provision the SEND-RDN-AS-CPN token for various call-redirection scenarios and results.

Figure 3-2 General Network View for Redirection by a Subscriber Phone

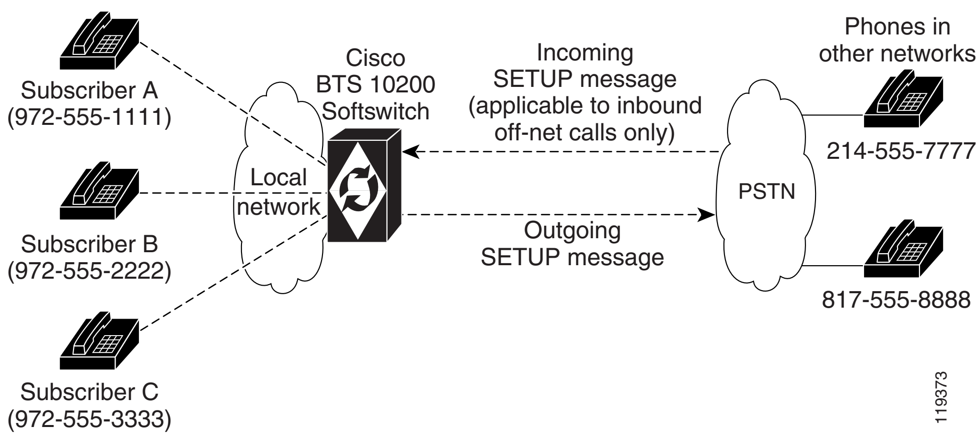


Table 3-4 Provisioning SEND-RDN-AS-CPN Token in TRUNK-GRP Table for Redirection by a Subscriber Phone

Scenario (See Figure 3-2)	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
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

Figure 3-3 shows an example of the networks and phones involved in redirection of a basic or Tandem call. Table 3-5 explains how to provision the SEND-RDN-AS-CPN token for call-redirection scenarios and results. Note that the content of the outbound SETUP message depends on whether the RDN is available in the incoming SETUP message.

Figure 3-3 General Network View for Redirection of Basic or Tandem Call

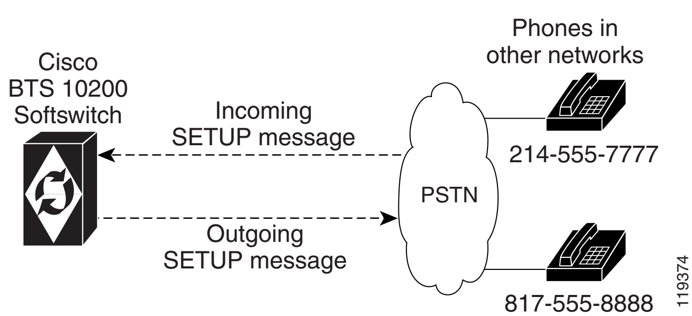


Table 3-5 Provisioning SEND-RDN-AS-CPN Token in TRUNK-GRP Table for Redirection of Basic or Tandem Call

Scenario (See Figure 3-3)	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 off-net call (basic or Tandem) with RDN available in the incoming SETUP message: off-net call -> Cisco BTS 10200 Softswitch -> off-net	CPN= 214-555-7777 RDN= 817-555-8888 (from incoming SETUP message)	Y	Overwrite CPN with RDN	CPN= 817-555-8888 RDN= 817-555-8888
		N	Do not change CPN	CPN= 214-555-7777 RDN= 817-555-8888
Off-net to off-net call (basic or Tandem) with RDN *not available* in the incoming SETUP message: off-net call -> Cisco BTS 10200 Softswitch -> off-net	CPN= 214-555-7777 *RDN not available* (from incoming SETUP message)	Y	Do not change CPN	CPN= 214-555-7777 RDN not available
		N	Do not change CPN	CPN= 214-555-7777 RDN not available

Tip To view all the tokens in this table, see the Trunk Group Table information in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

Dialing Parity (IntraLATA Toll Presubscription)

The Cisco BTS 10200 Softswitch 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.

Lawful Intercept Interface

This section describes the lawful intercept interface supported by the Cisco BTS 10200 Softswitch.

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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch described below may also be subject to change over time.

Note 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 Cisco BTS 10200 Softswitch 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).

Lawful Intercept Call Data Interface

The Cisco BTS 10200 Softswitch 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-EM-I08-040113, *PacketCable Event Messages Specification (EMS),* January 13, 2004.

Full call-identifying information (call data) is shipped to a DF server from the Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch searches for a PacketCable-compliant call-content intercept access point (IAP) in the call path. If the Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch. The Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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.

Local Number Portability (LNP)

The Cisco BTS 10200 Softswitch supports the local number portability (LNP) feature. For further 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 Cisco BTS 10200 Softswitch using the default office service ID. See the "Default Office Service ID" section on page 4-72 for a general description of this provisionable service.

Note For a complete description of the LNP feature and the applicable provisioning procedures, see the *Local Number Portability* feature module in the Cisco BTS 10200 Softswitch documentation set.

The Cisco BTS 10200 Softswitch supports the LNP function as follows:

- Ranges/blocks of ported numbers are provisionable in the Cisco BTS 10200 Softswitch, 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 Cisco BTS 10200 Softswitch 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 GenericAddress 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".

Network Loopback Test for NCS/MGCP Subscriber Endpoints

This feature allows support for a network loopback test on any MGCP/NCS subscriber endpoints controlled by the Cisco BTS 10200 Softswitch. With Release 4.4.x, the system supports line-side testing only. The procedure for setting up the test includes configuring the test lines as subscriber terminations and provisioning the MGW parameters. The procedure is described in the *Release Notes* document.

The following limitations apply:

- The testing and tested devices must be configured on same Call Agent.
- The system does not support loopback testing across a SIP or H.323 network.

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 Cisco BTS 10200 Softswitch. 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 Cisco BTS 10200 Softswitch. 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 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*.

T.38 Fax Relay

The Cisco BTS 10200 Softswitch communicates with MGWs to permit faxes to be transported across the IP network in the MGCP and H.323 control environments. The process is based on the following standards documents:

- IETF document *RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*
- ITU-T Recommendation *T.38 (06/98) - Procedures for Real-Time Group 3 Facsimile Communication Over IP Networks*

The system supports three fax modes:

- T.38 CA-controlled mode—This mode can be used for either of the following fax scenarios:
  - Faxes transmitted between a Cisco IOS MGCP-based MGW and an H.323 gateway (GW)
  - Faxes transmitted between two MGCP-based MGWs

  In T.38 CA-controlled mode, the CA instructs the gateway to switch to T.38 fax mode in real time. The CA receives a signal (Request mode for H.323 and Notify(fax) for MGCP) when fax signaling starts and stops. The CA maps the fax messages according to the protocol (MGCP or H.323) used for the originating and terminating messages. Billing records are generated in the CA based on fax start and stop signals. For information, see industry standards documents on H.323 Annex D version 2 (also incorporated into H.323 version 4) and MGCP FXR package.
- T.38 MGW-controlled mode—This mode can be used only for faxes transmitted between two Cisco IOS MGCP-based MGWs. In this mode, the CA passes the Session Description Protocol (SDP) information between the MGWs as in a normal voice call, and the CA is unaware that SDP extensions are being used by the MGWs for T.38 fax relay. After the SDP is exchanged, and if the MGW detects the fax call, it negotiates the codec to invoke the T.38 fax procedure automatically without CA involvement. The MGWs communicate with each other by using the RTP name signaling event (NSE) mechanism to exchange information.
- Inband Mode—This mode can be used for fax transmissions between two H.323 GWs, or between two MGCP MGWs. In this mode, the fax tones exchange is done directly over voice codec (G.711 or G.726 only). The CA treats this as it would any voice call.

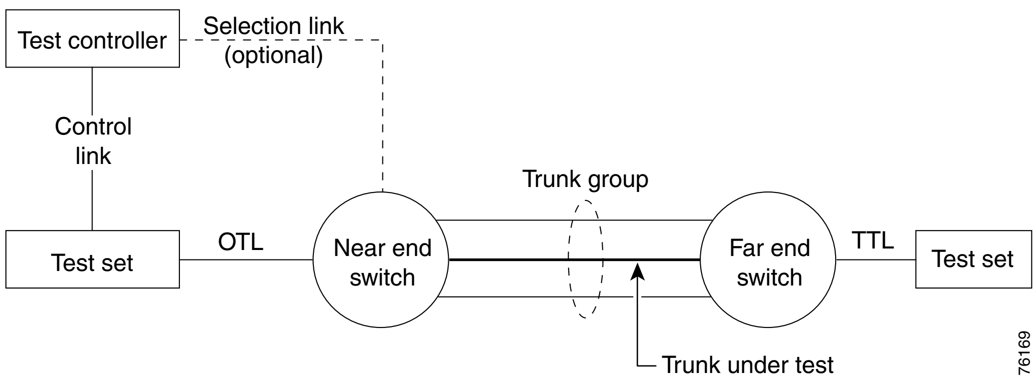
Trunk Testing

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 3-4.

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

Figure 3-4 Trunk Testing Setup



Near End Test Origination Test Calls

The Cisco BTS 10200 Softswitch supports calls used to test individual trunks that connect a local gateway with a gateway or PSTN switch at a remote office. The Cisco BTS 10200 Softswitch 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.

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

The process for testing a Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch.
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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch, the user can dial the test type with the 9581 or 9591 included: *KP-00030018-9581104-ST.*

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

T108 Test Line Support

The T108 test line feature determines the performance of trunks connecting digital exchange switches, including voice over packet (VoP) softswitches. Cisco BTS 10200 Softswitch 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 3-4.
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.

Note 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.

CHAPTER 4

Subscriber Features

Revised: March 19, 2007, OL-5906-14

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, Cisco BTS 10200 Softswitch 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:

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

Note For network features, see Chapter 3, "Network Features." For outgoing call restriction options (Class of Service and Outgoing Call Barring), see Chapter 5, "Class of Service Restrictions and Outgoing Call Barring."

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 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 Cisco BTS 10200 Softswitch. (These values are listed in the Vertical Service Code appendix of the *Cisco BTS 10200 Softswitch Command Line Interface Reference 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 the appendix of the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Subscriber Feature List

Table 4-1 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 4-1 Subscriber Features

Feature Description	Industry Reference Document	Subscriber Category
Call Forwarding Features		
• Call Forwarding Unconditional (CFU) • Special CFU-Related Functions – Call Forwarding Variable for Basic Business Group (CFVBBG) – Remote Activation of Call Forwarding (RACF) – Remote Call Forwarding (RCF)	FSD 01-02-1401 GR-580 FSD 01-02-1450 GR-586 FSD 01-02-1450 GR-586	Centrex POTS
Call Forwarding Busy (CFB)	FSD 01-02-1450 TR-TSY-000586	Centrex POTS
Call Forwarding No Answer (CFNA)	FSD 01-02-1450 TR-TSY-000586 FSD 01-02-2200 TR-TSY-001520	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

Table 4-1 Subscriber Features (continued)

Feature Description	Industry Reference Document	Subscriber Category
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
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
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

Table 4-1 Subscriber Features (continued)

Feature Description	Industry Reference Document	Subscriber Category
Automatic Callback (AC)—Repeat Dialing	GR-215-CORE	Centrex POTS
Automatic Recall (AR)—Call Return	GR-227-CORE	Centrex POTS
Call Block (Reject Caller)		Centrex POTS
Call Transfer (CT)	FSD 01-02-1305 TR-TSY-000579	Centrex POTS
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
Multiline Hunt Group (MLHG)	FSD 01-02-0802 TR-TSY-000569	Centrex POTS
Multiple Directory Numbers (MDN)		POTS only
Speed Call • Speed Call for Individual Subscribers • Group Speed Call (Centrex and MLHG only)	FSD 01-02-1101 TR-TSY-000570	Centrex POTS
Subscriber-Controlled Services and Screening List Editing	FSD 30-28-1000 GR-220-CORE	Centrex POTS
• Selective Call Forwarding (SCF)	FSD 01-02-1410 TR-TSY-000217	
• Selective Call Acceptance (SCA)		
• Selective Call Rejection (SCR)	FSD 01-02-0760 TR-TSY-000218	
• Distinctive Ringing/Call Waiting (DRCW)	FSD 01-01-1110 TR-TSY-000219	

Table 4-1 Subscriber Features (continued)

Feature Description	Industry Reference Document	Subscriber Category
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
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)
- Special CFU-Related Functions

Note The Special CFU-Related Functions section includes information on Call Forwarding Variable for Basic Business Group (CFVBBG), Remote Activation of Call Forwarding (RACF), and Remote Call Forwarding (RCF).

- Call Forwarding Busy (CFB)
- Call Forwarding No Answer (CFNA)

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 4-2.

Table 4-2 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 hopping 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 4-6
- CFU Deactivation (CFUD), page 4-8
- CFU Interrogation (CFUI), page 4-9
- CFU Invocation, page 4-9

CFU Activation (CFUA)

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

CFUA Customization Options

The behavior of CFU activation 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 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.

> **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.

- 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. If the SDT flag is set to Y, the system provides a second dial tone. If SDT is set to N, the system does not provide a second dial tone.

> **Note** For SIP phone subscribers, this dial tone will not be provided, even if the SDT flag is set.

- 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 the FDT flag is set to Y, the system provides a confirmation tone for one second, followed by a dial tone. If FDT is set to N, the system provides a success announcement.

> **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.)

Example—Using the Customization Options

The typical North America and China variants of the CFUA flags can be provided by configuring the options as follows:

- China—CC=N; SDT=N; FDT=N
- North America—CC=ANS; SDT=Y; FDT=Y

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 4-6 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 a stutter 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 a 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 4-6 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 a 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 4-6 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 a stutter 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 a 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 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 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, Maintenance, and Troubleshooting 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—COS takes precedence over CFU activation (CFUA and CFVABBG) and CFU invocation (CFU and CFVBBG). 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.

Special CFU-Related Functions

The Cisco BTS 10200 Softswitch supports the following special CFU-related functions:

- Call Forwarding Variable for Basic Business Group (CFVBBG), page 4-12—This feature is a special variant of CFU available only to BBGs with Centrex service. CFVBBG implements the following courtesy call treatment during activation:
  – When CFVBBG is activated to an extension, no courtesy call is placed.
  – When CFVBBG is activated to an outside line, a courtesy call is placed.
- Remote Activation of Call Forwarding (RACF), page 4-13—This feature allows the user to access an interactive voice response (IVR) system to activate CFU from a remote station.
- Remote Call Forwarding (RCF), page 4-13—This feature is set up by the service provider at customer request. It allows all incoming calls to a specified DN to be forwarded automatically to a forward-to DN. It is not controlled by the user with a handset.

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. 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 4-6 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, Maintenance, and Troubleshooting 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.
- 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.

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 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.

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 usually set up by the service provider at the subscriber's request.

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

Note When endpoint monitoring is disabled and the eMTA powered down, calls to subscribers on that eMTA are not forwarded to voicemail. Those calls are released with a release cause of 41 (Temporary Failure). If endpoint monitoring is enabled, call forwarding to voicemail works as expected. (This note does not apply to SIP subscribers; for SIP subscribers, calls can be forwarded when the SIP endpoint is unreachable or unregistered.)

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 4-3.

Table 4-3 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 hopping 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 4-15
- CFB Variable Deactivation (CFBVD), page 4-16
- CFB Interrogation (CFBI), page 4-17
- CFB Invocation, page 4-18

CFB Variable Activation (CFBVA)

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

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. If the SDT flag is set to Y, the system provides a second dial tone. If SDT is set to N, the system does not provide a second dial tone.

  Note For SIP phone subscribers, this dial tone will not be provided, even if the SDT flag is set.

- 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 the FDT flag is set to Y, the system provides a confirmation tone for one second, followed by a dial tone. If FDT is set to N, the system provides a success announcement.

  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.)

Example—Using the Customization Options

The typical North America and China variants of the CFBVA flags can be provided by configuring the options as follows:

- China—CC=N; SDT=N; FDT=N
- North America—CC=N; SDT=Y; FDT=Y

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 4-15 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 a stutter 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 a 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 4-15 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 a 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 4-15 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 a stutter 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 a 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 Feature Server (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 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, Maintenance, and Troubleshooting 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, Maintenance, and Troubleshooting 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—COS takes precedence over CFB activation (CFBVA) and CFB invocation (CFB). If a call to a DN is restricted by COS screening, CFB cannot be activated or invoked to that DN.

Call Forwarding No Answer (CFNA)

The Cisco BTS 10200 Softswitch 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 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.

Note 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 4-4.

Table 4-4 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 hopping 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 4-21
- CFNA Variable Deactivation (CFNAVD), page 4-22
- CFNA Interrogation (CFNAI), page 4-23

- CFNA Invocation, page 4-24

CFNA Variable Activation (CFNAVA)

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

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. If the SDT flag is set to Y, the system provides a second dial tone. If SDT is set to N, the system does not provide a second dial tone.

  Note For SIP phone subscribers, this dial tone will not be provided, even if SDT flag is set.

- 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 the FDT flag is set to Y, the system provides a confirmation tone for 1 second, followed by a dial tone. If FDT is set to N, the system provides a success announcement.

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

Example—Using the Customization Options

The typical North America and China variants of the CFNAVA flags can be provided by configuring the options as follows:

- China—CC=N; SDT=N; FDT=N
- North America—CC=N; SDT=Y; FDT=Y

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 4-21 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 a stutter 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 a 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 4-21 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 a 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 4-21 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 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 a 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 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 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, Maintenance, and Troubleshooting 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.
- 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.

  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 CFNA active simultaneously, the service provider should not assign the CHD feature to that subscriber.
- COS—COS takes precedence over CFNA activation (CFNAVA) and CFNA invocation (CFNA). If a call to a DN is restricted by COS screening, CFNA cannot be activated or invoked to that DN.
- 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. The CW (or CWD) feature does not perform any timing in this case. 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.
- CW—If both CFNA and CW 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 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.

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 4-26
- Cancel Call Waiting (CCW), page 4-28
- Calling Identity Delivery on Call Waiting (CIDCW), page 4-29
- Call Waiting Deluxe (CWD), page 4-31

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 Cisco BTS 10200 Softswitch 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 4-29.

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 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 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.

- 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.

  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 CFNA active simultaneously, the service provider should not assign the CHD feature to that subscriber.

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 4-29). 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 If a user was involved in a multiparty call, and received a ringback after going on hook, CCW remains active for the call.

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.

- 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.

Calling Identity Delivery on Call Waiting (CIDCW)

The Cisco BTS 10200 Softswitch 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.

  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 CFNA active simultaneously, the service provider should not assign the CHD feature to that subscriber.

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 4-67.)

- 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 4-32
- CWD Deactivation, page 4-33
- CWD Interrogation, page 4-33
- CWD Invocation, page 4-33

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.

Calling Identity Features

Calling identity features include:

- Calling Identity Delivery, page 4-35
  - Calling Number Delivery (CND), page 4-35
  - Calling Name Delivery (CNAM), page 4-35
- Calling Line Identification Presentation (CLIP), page 4-35
- Calling Identity Delivery Blocking (CIDB), page 4-37
  - Calling Number Delivery Blocking (CNDB), page 4-38
  - Calling Name Delivery Blocking (CNAB), page 4-38
  - Calling Identity Delivery and Suppression (CIDSD and CIDSS), page 4-39

Note The calling identity delivery on call waiting (CIDCW) feature is described in the "Call Waiting Features" section on page 4-26.

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 Cisco BTS 10200 Softswitch 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.

Calling Name Delivery (CNAM)

The Cisco BTS 10200 Softswitch 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.

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.

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 (Cisco BTS 10200 Softswitch) 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 (Cisco BTS 10200 Softswitch) 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 4-5 and described in the "Calling Number Delivery Blocking (CNDB)" section on page 4-38 through the "Calling Identity Delivery and Suppression (CIDSD and CIDSS)" section on page 4-39.

Note The vertical service codes (VSCs), also called star codes, listed in Table 4-5 and throughout this section are typical values. The service provider can provision these values with any unique ASCII string up to five characters long. For a complete list of preprovisioned VSCs, see the VSC appendix in the *Cisco BTS 10200 Softswitch CLI Reference Guide*.

Table 4-5 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.

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.

Calling Identity Delivery and Suppression (CIDSD and CIDSS)

The Cisco BTS 10200 Softswitch 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.

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 4-35.

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 4-41
- Calling Name Delivery Blocking (CNAB), page 4-41
- Calling Identity Delivery and Suppression (CIDSD and CIDSS), page 4-42

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 4-6 and described in the "Calling Number Delivery Blocking (CNDB)" section on page 4-41 through the "Calling Identity Delivery and Suppression (CIDSD and CIDSS)" section on page 4-42.

Note The vertical service codes (VSCs), also called star codes, listed in Table 4-6 and throughout this section are typical values. The service provider can provision these values with any unique ASCII string up to five characters long. For a complete list of preprovisioned VSCs, see the VSC appendix in the *Cisco BTS 10200 Softswitch CLI Reference Guide*.

Table 4-6 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.

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.

Calling Identity Delivery and Suppression (CIDSD and CIDSS)

The Cisco BTS 10200 Softswitch 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.

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.

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

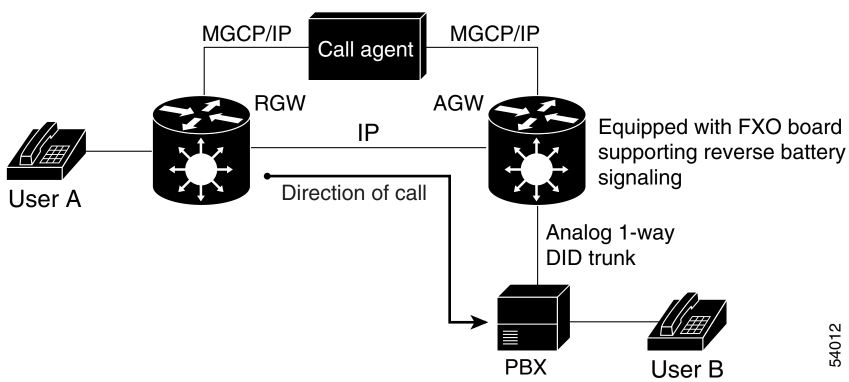
The Cisco BTS 10200 Softswitch supports analog DID for PBX as specified in TIA/EIA-464B, *Requirements for Private Branch Exchange (PBX) Switching Equipment*, April 1, 1996.

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 4-1 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 4-1 Example of PBX Analog DID One-Way Application



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.

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.

The following features are available to Centrex subscribers only:

- Call Hold (CHD), page 4-44
- Call Park and Call Retrieve, page 4-45
- Direct Inward/Outward Dialing for Centrex, page 4-45
- Directed Call Pickup (With and Without Barge-In), page 4-46
- Distinctive Alerting/Call Waiting Indication (DA/CWI), page 4-47

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.

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.
- 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.

   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 CFNA active simultaneously, the service provider should not assign the CHD feature to that subscriber.

- 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.

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 hears either music-on-hold or silence. 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.

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 ringing for DID
- DOD

DID for Centrex with Distinctive Ringing

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.

The Cisco BTS 10200 Softswitch supports distinctive ringing for DID. The service provider can provision the distinctive ringing feature for Centrex customers. When enabled (da-cwi=yes in the centrex-grp table), the customers within the Centrex group will be able to 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)
  - 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 Incoming calls originating from a *different* Centrex are treated as outside calls.

DOD for Centrex

The Cisco BTS 10200 Softswitch supports the DOD feature. 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)

Note This feature is available only to 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

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.

Additional Features Applicable to Centrex and POTS

The following additional features are available to both Centrex and POTS subscribers:

- Anonymous Call Rejection (ACR), page 4-48
- Automatic Callback (AC)—Repeat Dialing, page 4-49
- Automatic Recall (AR)—Call Return, page 4-49
- Call Block (Reject Caller), page 4-51
- Call Transfer (CT), page 4-51

Anonymous Call Rejection (ACR)

The Cisco BTS 10200 Softswitch 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 offhook.

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.

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.

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.

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.*

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.

Call Block (Reject Caller)

The call block (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 4-65.

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, 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.

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.

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 Cisco BTS 10200 Softswitch for retrieval purposes. A maximum of 10,000 traces are stored in a circular file format (oldest record overwritten).

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.

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:

- None of the VSC star (*) features are available on this line
- The user cannot originate additional outgoing calls by pressing the Flash button or hookswitch. Therefore, the user will not be able to originate multiparty or conference calls from the hotline phone.

Only the service provider can deactivate hotline service.

Note See also the "Warmline Service" section on page 4-72. Warmline service is a combination of hotline service and regular phone service.

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 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.

Certain limitations apply to hotline calls:

- None of the VSC star (*) features are available on this line, other than the VSC codes for hotline-variable activation, deactivation, and interrogation.

- The user cannot originate additional outgoing calls by pressing the Flash button or hookswitch. Therefore, the user will not be able to originate multiparty or conference calls from the hotline phone.

This remote DN is referred to as the B-number. The allowed types of B-numbers are listed in Table 4-7.

Table 4-7 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 4-54
- Hotline-Variable Deactivation, page 4-54
- Hotline-Variable Interrogation, page 4-55
- Hotline-Variable Invocation, page 4-55

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.

Interactive Voice Response (IVR) Functions

The Cisco BTS 10200 Softswitch supports interactive voice response (IVR) functions for activation of remote call forwarding (RACF) and screening list editing (SLE) features. To use the RACF feature, the user dials a specified 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 their RACF options. To use the SLE feature, the user dials one of several VSC (*xx) numbers and is connected to the appropriate IVR media server. The user follows the voice prompts to edit their screening lists.

For additional details of these features, refer to the following sections:

- Remote Activation of Call Forwarding (RACF), page 4-13
- Subscriber-Controlled Services and Screening List Editing, page 4-63

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.

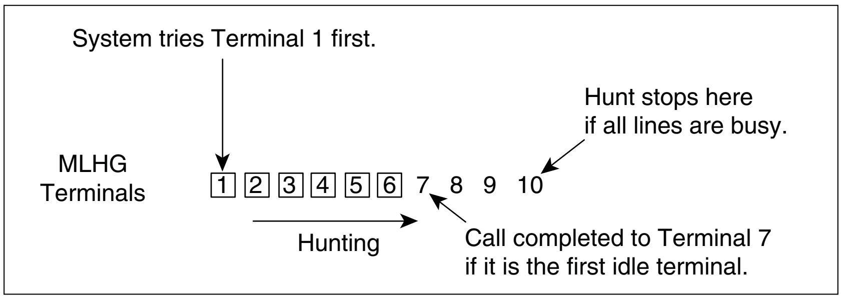
The starting point for the hunt depends upon whether the incoming call is being routed to the group or to the individual. These scenarios are described in the following sections:

- Incoming Call to the Pilot DN, page 4-57
- Incoming Call to an Individual DN, page 4-58

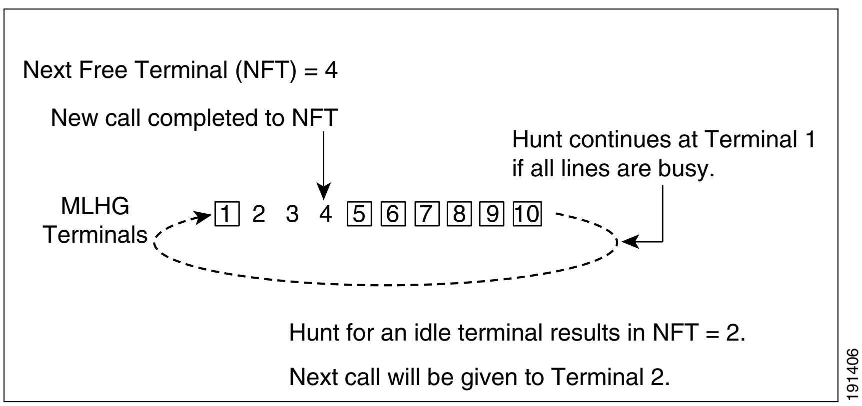
Incoming Call to the Pilot DN

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 4-2 illustrates this process.

Figure 4-2 Searching an MLHG—Incoming Call to the Pilot DN (Example)



Regular hunt and circular hunt



UCD hunt

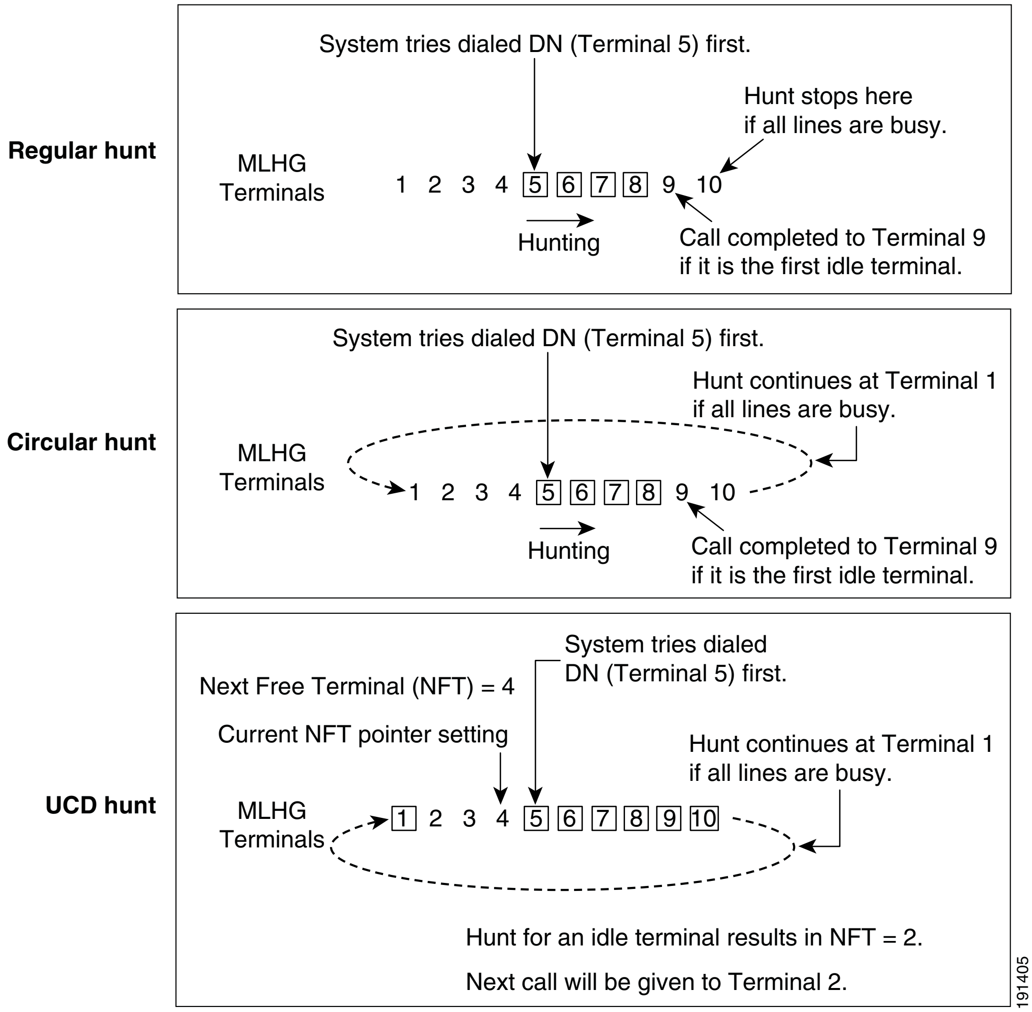
Notes for Figure 4-2

- A rectangle surrounding a number means the line is busy.
- Regular hunt and circular hunt—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 4-3 illustrates this process.

Figure 4-3 Searching an MLHG—Incoming Call to an Individual Terminal (Example)



Notes for Figure 4-3

- 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.

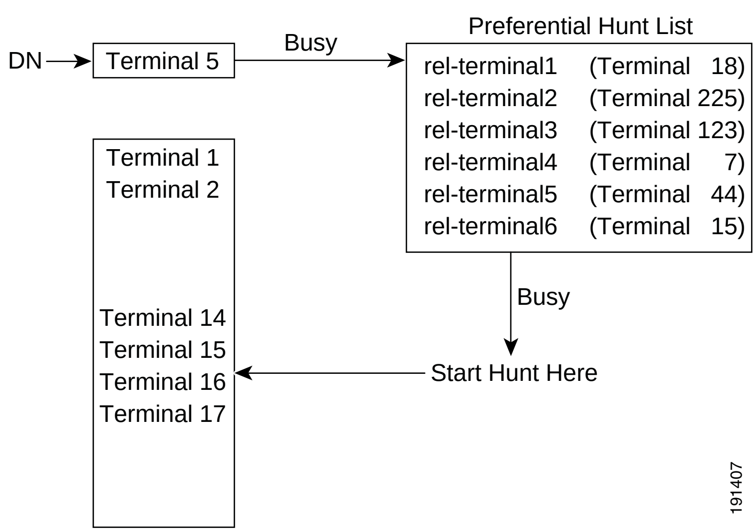
- UCD hunt—The incoming call is routed to the terminal with the dialed DN, Terminal 5 in this example. If Terminal 5 is idle, the system completes the call to Terminal 5 and does not attempt to change the NFT pointer. If Terminal 5 is busy, the system completes the call to the NFT. In this example, the 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.
- Special case for UCD (not shown in the drawing)—If the dialed DN is idle and receives the call, the system checks whether this terminal already has the NFT pointer. If so, the system performs a hunt for the next idle terminal and assigns the NFT to that idle terminal.
- 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 4-59. 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 4-4.

Note The system does *not* invoke the preference list (preferential hunt) if hunt-type=UCD in the MLHG table.

Figure 4-4 Searching a Preferential Hunt List (Example)



MLHG Provisioning Options and Use Cases

Table 4-8 explains how provisioning in the Subscriber table affects the behavior of a terminal in the MLHG.

Table 4-8 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 subscriber::category 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.

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.

Call forwarding—If call forwarding busy (CFB) is assigned and active for the main subscriber, and if all terminals in the MLHG are busy, an incoming call to the pilot number receives CFB treatment. However, if the incoming call is to an *individual DN*, and that DN is busy, the treatment depends on the provisioning for that individual subscriber record:

- If the individual subscriber record has grp=Y, and the main subscriber has CFB assigned and active, the call receives CFB treatment. (The individual subscriber inherits the CFB feature from the main subscriber.)
- If the individual subscriber has grp=N, but has CFB assigned as an individual feature, the call receives CFB treatment as provisioned for the individual.
- If CFB is not assigned to this subscriber, either by inheritance or by individual assignment, the incoming call receives busy treatment without forwarding.

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).
- 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.

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 "Multiline Hunt Group" chapter of the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide.*

Multiple Directory Numbers (MDN)

Multiple directory numbers (MDN) service is also known as teen service. It enables one primary DN and one or two 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.

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 offhook 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.

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.

Subscriber-Controlled Services and Screening List Editing

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)
- 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*. The user performs the SLE functions, and activates/deactivates the services, via VSCs. Each VSC connects the user to the appropriate 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 following sections.

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.

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 4-6.

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)" section on page 4-51) 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 SCR 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.

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 4-67).

> **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.

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 4-70).
- 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.

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 4-66) 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.

Visual Message Waiting Indicator (VMWI)

The visual message waiting indicator (VMWI) is associated with the voice mail service. When a call is forwarded to a voice mail system, and the caller leaves a message, the voice mail system sends the Cisco BTS 10200 Softswitch an MWI signal via SIP. The Cisco BTS 10200 Softswitch forwards a VMWI signal to the called party, and the called party's telephone indicator light turns on. When the called party retrieves the message, the voice mail system signals the Cisco BTS 10200 Softswitch to clear the VMWI indicator, and the light on the telephone turns off.

Warmline Service

Warmline service is a combination of hotline service (see the "Hotline Service" section on page 4-53) 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.

An exclusive telephone DN is required for the warmline feature, and certain limitations apply to its use:

- None of the VSC star (*) features are available on this line
- The user cannot originate additional outgoing calls by pressing the Flash button or hookswitch. Therefore, the user will not be able to originate multiparty or conference calls from the warmline phone.

Only the service provider can deactivate warmline service

Default Office Service ID

One service ID (the default office service ID) is reserved for provisioning of switch-based features. These switch-based features can include certain network features and certain usage-sensitive features, as described below. The service provider enters a unique ID (DEFAULT-OFFICE-SERVICE-ID) in the CA-CONFIG table, provisions this service ID in the SERVICE table, and defines these features in the FEATURE table.

Note Refer to the *Cisco BTS 10200 Softswitch Provisioning Guide* for specific feature provisioning requirements.

Caution The system does not validate or restrict the provisioning of features on this 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.

- Network features—When provisioned, the system makes these features available for all subscriber lines:

  Note See Chapter 3, "Network Features" for details of these network features.

  - Local network portability (LNP)
  - Toll-free services (8XX)
  - Emergency services (911)
  - Busy line verification (BLV)
- Usage-sensitive features—When provisioned, the system makes these features available to all subscribers without the need to actually subscribe these features to individual lines:

  Note These features can also be assigned to individual subscribers using other service IDs.

  - Usage-sensitive three-way calling (USTWC)
  - Customer originated trace (COT)
  - Automatic callback activation and deactivation—AC_ACT and AC_DEACT (or AC, if the AC umbrella feature was created)
  - Automatic recall activation and deactivation—AR_ACT and AR_DEACT) (or AR, if the AR umbrella feature was created)

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 5

Class of Service Restrictions and Outgoing Call Barring

Revised: March 19, 2007, OL-5906-14

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 Restrictions
- Outgoing Call Barring (OCB)

Note For information on network features, see Chapter 3, “Network Features.”

For information on subscriber features, see Chapter 4, “Subscriber Features.”

Class of Service Restrictions

The Cisco BTS 10200 Softswitch supports class of service (COS) restrictions on certain call types. 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. When a call is blocked, the calling party receives a blocking treatment such as reorder tone or announcement. Number blocking is activated/deactivated and administered by the service provider on a per-line or per-group-of-lines basis. The service provider can prohibit calls based on dialing plans and call types.

Certain types of calls are exempt from COS and OCB restrictions:

- Emergency calls
- Call types on the NOD exception list (NOD restrict list)—The service provider can provision an exception list to override COS and OCB screening on certain types of calls. The types of calls on this list can include, for example, emergency calls, toll-free calls, and so forth. The applicable types of calls are listed in the NATURE-OF-DIAL (NOD) table, and the specific exceptions are provisioned in the NOD-RESTRICT-LIST table. These exceptions are applicable at the switch level (all office codes) and cannot be specified for individual subscribers.

  Note A complete list of NOD values is provided in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

This section covers the following topics:

- National Call Restrictions (Toll Restrictions)
- 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 (Number Blocking)
- Nature of Dial White and Black Lists (Number Blocking)
- Blocking Flags
- Account Codes and Authorization Codes
- ANI Screening on Incoming Calls
- COS Restriction Priorities
- High-Level Flowchart of COS Screening Process

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.

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 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. The 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.

International calls within NANP will be 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 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 (Number Blocking)

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 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 (Number Blocking)

The nature of dial (NOD) white and black lists are used to allow or block certain categories of calls, such as casual dialing (dialing around), time/weather, international operator assistance, premium 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.

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.

Tip All call types can be placed on the NOD White Black List.

Note 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 Cisco BTS 10200 Softswitch supports account code and authorization code features as described in this section.

Note The system does not support account and authorization codes for ISDN trunks in this release.

Account Codes (Nonverified)

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

The system has a provisionable token that can be used to introduce delay (up to one second) before playing the account-code prompt.

Authorization Codes (Verified Account Codes)

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.

Note 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.

The system has a provisionable token that can be used to introduce delay (up to one second) before playing the authorization-code prompt.

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, 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 Cisco BTS 10200 Softswitch 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.

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.

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 5-1 and Figure 5-2 show a high-level flowchart of the COS screening process. The flowchart is split into two parts (two drawings) for easier viewing.

Figure 5-1 COS Screening Process (Part 1)

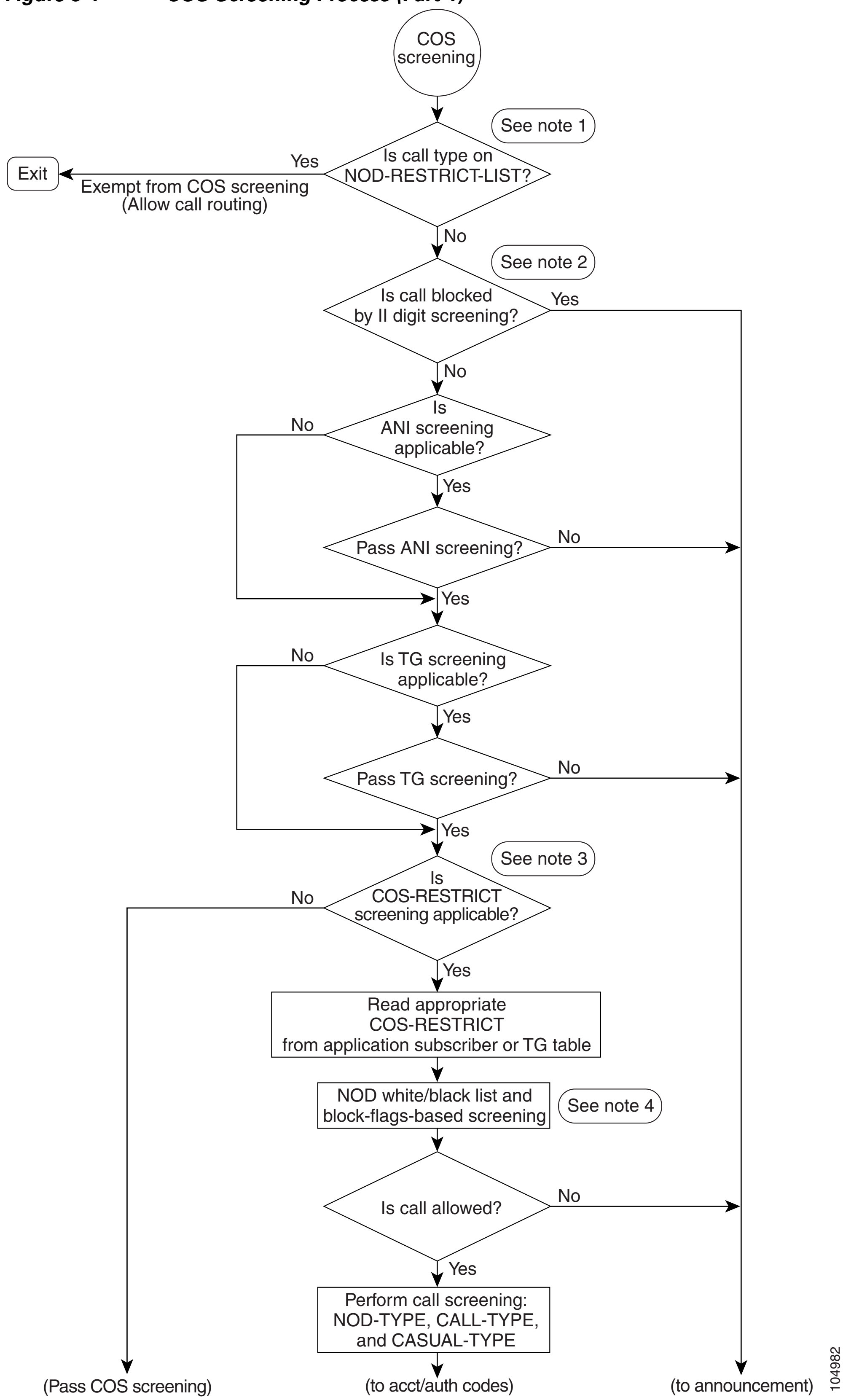
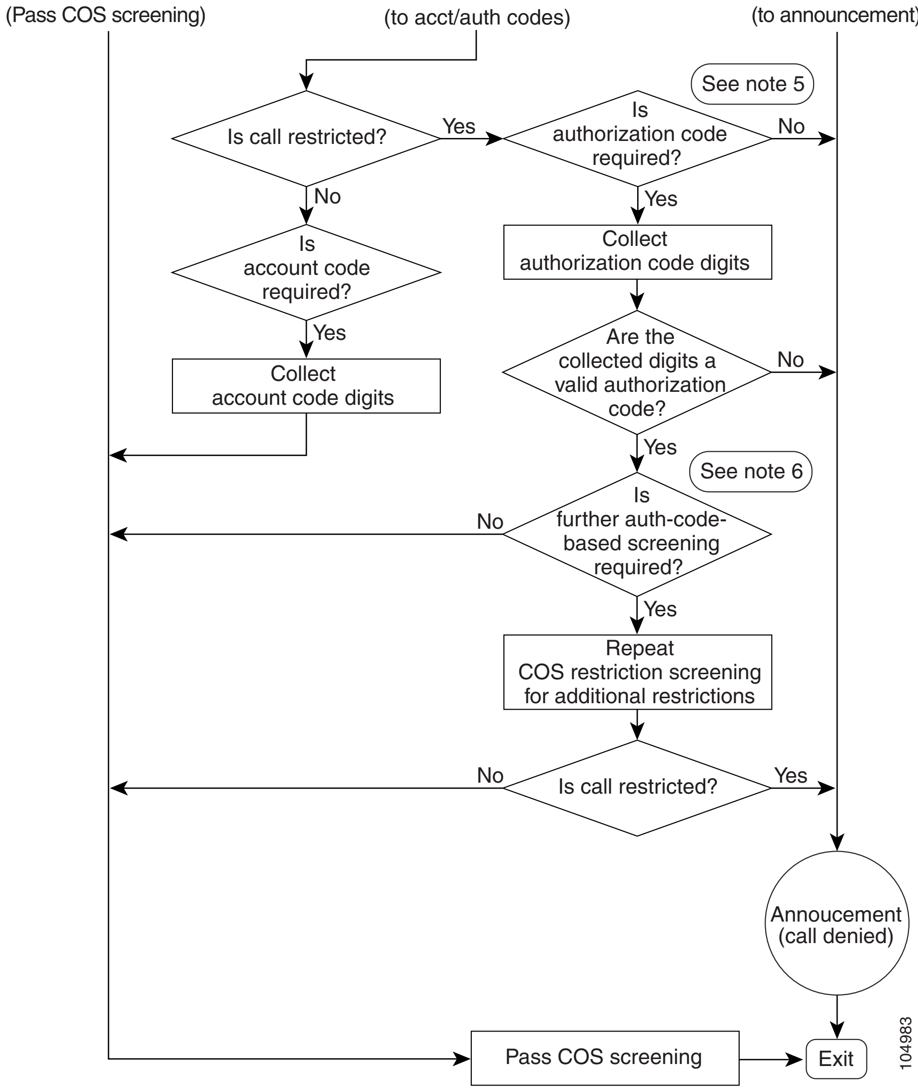


Figure 5-2 COS Screening Process (Part 2)



Notes for Figure 5-1 and Figure 5-2:

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)

The outgoing call barring (OCB) feature allows an individual subscriber or business group administrator to restrict certain types of outgoing calls. Once the OCB feature is provisioned and activated on a calling line, the OCB restrictions are transparently invoked on all outgoing calls.

This section covers the following topics:

- OCB Subscription and Provisioning
- OCB Activation and User Options
- OCB Deactivation
- OCB Interrogation
- OCB Invocation and Screening
- Class of Service Screening via Black and White List
- OCB Feature Interactions

Note For Release 4.4.1, the OCB feature has been enhanced with additional provisionable options. If your system is running Release 4.4.1, and you would like to use those additional options, see the *Enhanced Outgoing Call Barring* feature module in the Cisco BTS 10200 Softswitch documentation set.

Note 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.

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 (for example, *54*, #54* and *#54#).

  Note The VSCs used throughout this document are typical values. The service provider can provision these values with any unique ASCII string up to five characters long. For a complete list of preprovisioned VSCs, see the Vertical Service Code appendix in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

- Personal 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.
- PIN length (PIN-LEN)—The number of digits required for a valid PIN (can be provisioned as 1 to 8 digits).

  Note The PIN and PIN-LEN are provisioned by the service provider. They cannot be provisioned by the user via the handset, and cannot be changed by the user.

- Allowed activation/deactivation attempts and lockout parameters—Parameters can be provisioned to limit the number of times that a user can enter incorrect data or 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).

Detailed provisioning steps for these options are provided in the *Cisco BTS 10200 Softswitch Provisioning Guide*. Additional reference information on the provisionable parameters is available in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

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 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:
  - K-VALUE=1: all outgoing calls barred
  - K-VALUE=2: domestic long-distance and international outgoing calls barred
  - K-VALUE=3: international outgoing calls barred
- <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 only when the OCB feature is in the deactivated state.

If a user enters incorrect data or 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 5-11.

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 1, 2, or 3.
- The user enters an incorrect PIN.
- The user is not provisioned for the OCB feature.

OCB Deactivation

OCB deactivation (OCBD) allows 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 1, 2, or 3. However, the actual value is ignored by the system, because OCBD deactivates all call barring.
- <PIN> is the same as for OCBA.

A success announcement is given on a successful deactivation, and an error announcement, indicating the type of error, is given if deactivation is unsuccessful.

Note Refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for provisioning details.

If a user enters incorrect data or 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 5-11.

OCB Interrogation

OCB interrogation allows a user to check the level of outgoing call restrictions on the handset. The default 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, OCB is invoked for every call made after the called party digits are dialed.

OCB Lockout Behavior

The LOCK-OUT, TO (timeout), and FAIL-CNT (fail count) tokens in the feature table are intended to prevent unauthorized changes or bypassing of OCB screening. If a user repeatedly enters the password or other OCBA/OCBD data incorrectly on the handset, the system can lock the line against both OCBA and OCBD. These tokens control the lockout behavior as described in Table 5-1.

Tip Note that there is no service lockout when either the TO or FAIL-CNT token is set to zero.

Table 5-1 OCB Lockout Behavior

OCB Tokens in Feature Table			Lockout Behavior Due to OCBA/OCBD Misuse
LOCK-OUT	TO	FAIL-CNT	
—	—	0	No service lockout
—	0	—	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

Class of Service Screening via Black and White List

The Cisco BTS 10200 Softswitch supports class of service (COS) screening, which is provisioned and assigned by the service provider, and cannot be controlled or deactivated by individual subscribers. 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.
- White-listed calls are subject to additional normal OCB restrictions based on call type.

  Note The service provider provisions the desired COS restrictions for all subscribers that have the OCB feature. This ensures that the black and white list restrictions are in effect, even if the user deactivates OCB.

Note Separate black and white lists are maintained for local/national calls and international calls.

- National White Black Lists are used to allow or restrict calls to specified destinations within a region or within a local area.

  Note A region is a country or numbering plan area. The national White Black List identifies a set of national destination codes (NDCs) and/or exchange codes (ECs) to be allowed or blocked.

  Outgoing calls are restricted as follows:

  - No restrictions (default), except that all calls are subject to the additional OCB restrictions.
  - National white list—Allows calls within a predefined list, except that all calls are subject to the additional OCB restrictions.
  - National black list—Blocks all calls within a predefined list.

  Note National call restrictions do not apply to operator calls. This is true even if national call restriction is provisioned in the cos-restrict table for the calling party.

- International black/white lists are used to allow or restrict calls made to specific country codes. Outgoing calls are restricted as follows:

  - No international calls allowed—Does not allow any international calls
  - International white list—Allows those calls that have a prefix noted in the white list, except that all calls are subject to the additional OCB restrictions
  - International black list—Does not allow any calls that have a prefix noted in the black list
  - All international calls allowed—No restrictions are applied on any international calls, except that all calls are subject to the additional OCB restrictions

  Note International call restrictions do not apply to operator calls. This is true even if international call restriction is provisioned in the cos-restrict table for the calling party.

The service provider can provision an exception list to override COS and OCB screening on certain types of calls. The types of calls on this list can include, for example, emergency calls, toll-free calls, and so forth. The applicable types of calls are listed in the NATURE-OF-DIAL (NOD) table, and the specific exceptions are provisioned in the NOD-RESTRICT-LIST table. These exceptions are applicable at the switch level (all office codes) and cannot be specified for individual subscribers.

Note A complete list of NOD values is provided in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

OCB Feature Interactions

The section describes the interactions of OCB with other features.

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, or CFNA.

- 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.

Interaction with COS Restriction

The COS feature is an optional functionality (subset) of OCB. To use the COS functionality, the service provider must provision individual COS restriction settings for the subscriber line. Table 5-2 lists additional details about the interaction of COS and OCB.

Table 5-2 Interactions between COS and OCB Features

Desired Screening Function(s) On Outgoing Calls	Feature that Must Be Provisioned in Feature Table	Provisioning Required for COS Tables [1]	How the System Reports Billing Data
User-controlled screening only	OCB	Do not provision individual COS restrictions. Leave all COS table tokens set to their default values.	OCB
User-controlled screening and network (office) screening	OCB [2]	Provision individual COS restriction tables.	OCB
Network (office) screening only	COS	Provision individual COS restriction tables.	COS

1. The COS restriction tables include the following: COS-RESTRICT, NATIONAL-WB-LIST, INTL-WB-LIST, NOD-RESTRICT-LIST, and NOD-WB-LIST.
2. The COS feature is contained in the OCB feature.

CHAPTER 6

Feature Interactions

Revised: March 19, 2007, OL-5906-14

This chapter describes the interactions among the various features offered by the Cisco BTS 10200 Softswitch. It includes the following topics:

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 3, "Network Features" and Chapter 4, "Subscriber Features" for detailed descriptions of individual features.

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)

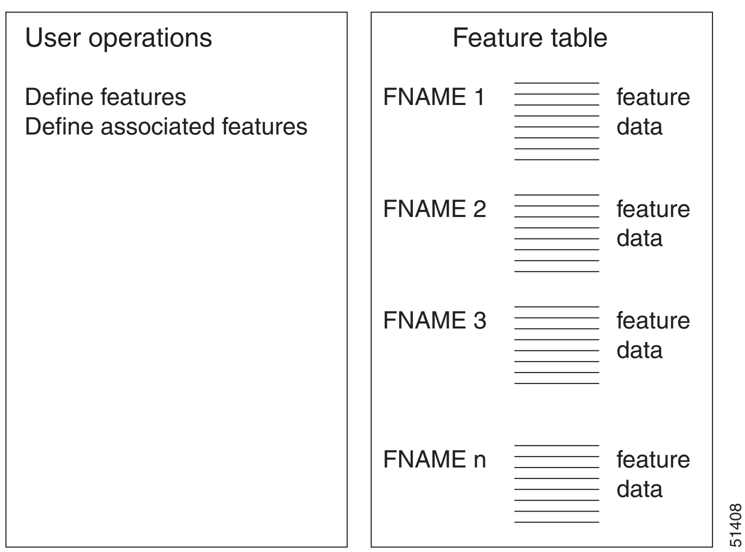
A service is a collection of one or more features (up to 10 features per service). Each service is identified by a unique service ID numeric value. Each feature within a service may have one or more triggers. When a service is created, the system automatically registers the triggers. During call processing, 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 6-1 through Figure 6-3 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 6-1 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 6-2 Assigning Features to Services

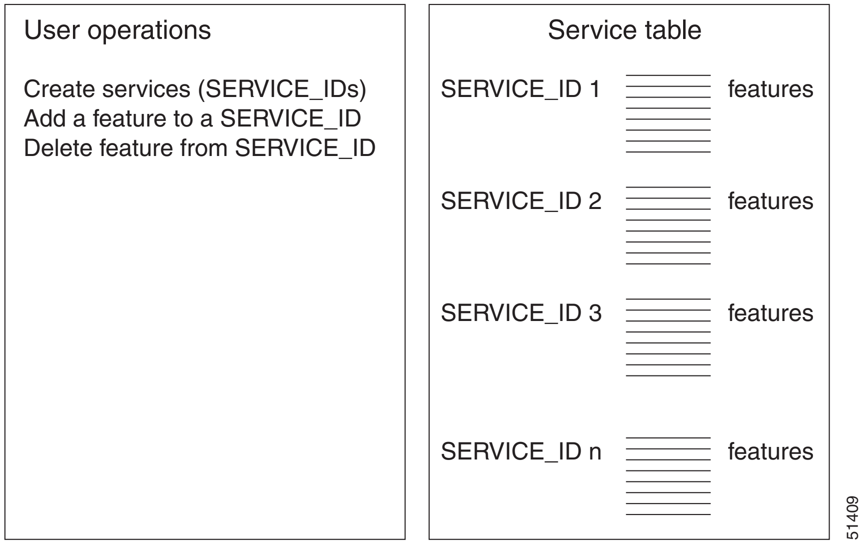
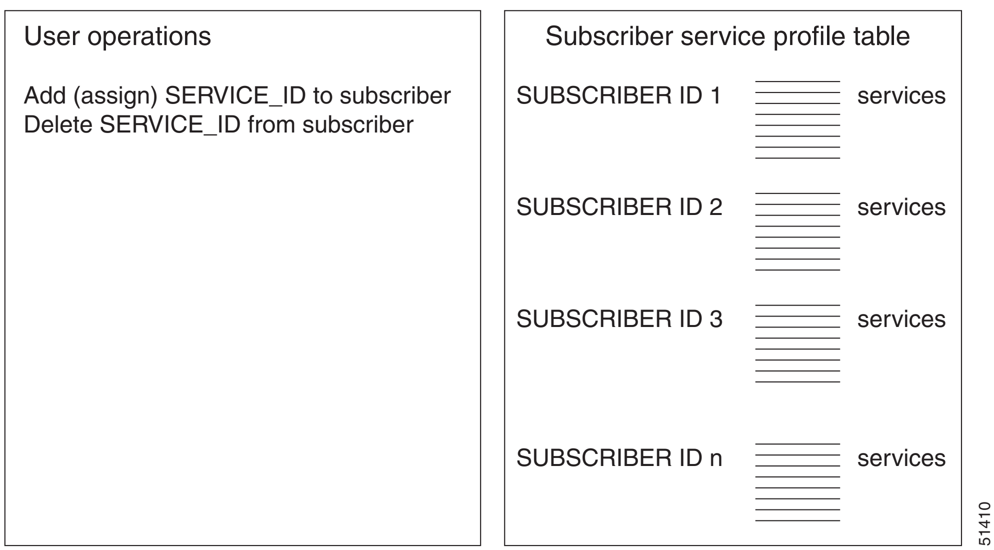


Figure 6-3 Assigning Services to Subscribers



Trigger Detection Points and Trigger IDs

The TDPs for the Cisco BTS 10200 Softswitch are illustrated in Figure 6-4 and Figure 6-5.

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.

Figure 6-4 Cisco BTS 10200 Softswitch Originating Call States and Triggers

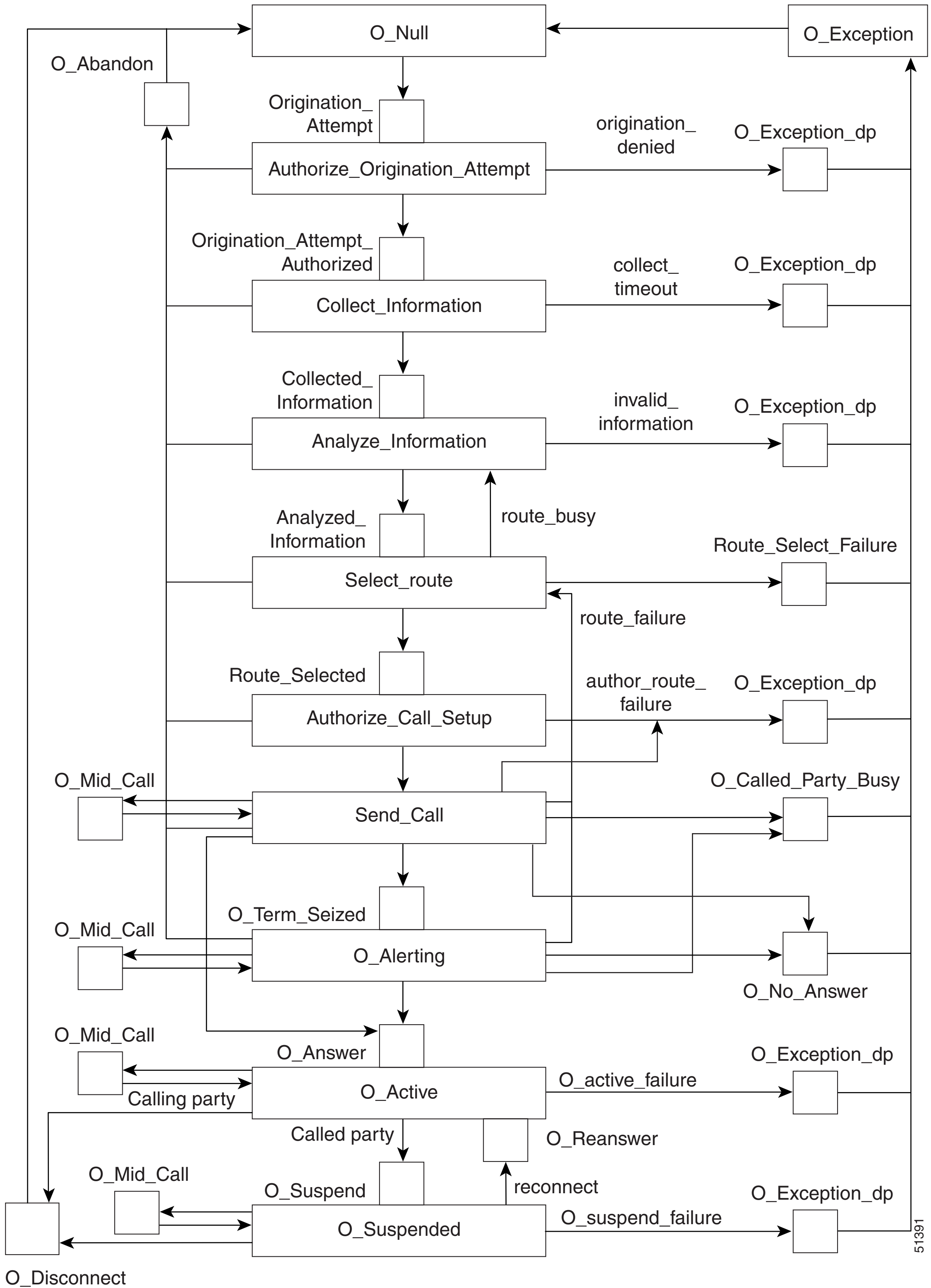


Figure 6-5 Cisco BTS 10200 Softswitch Terminating Call States and Triggers

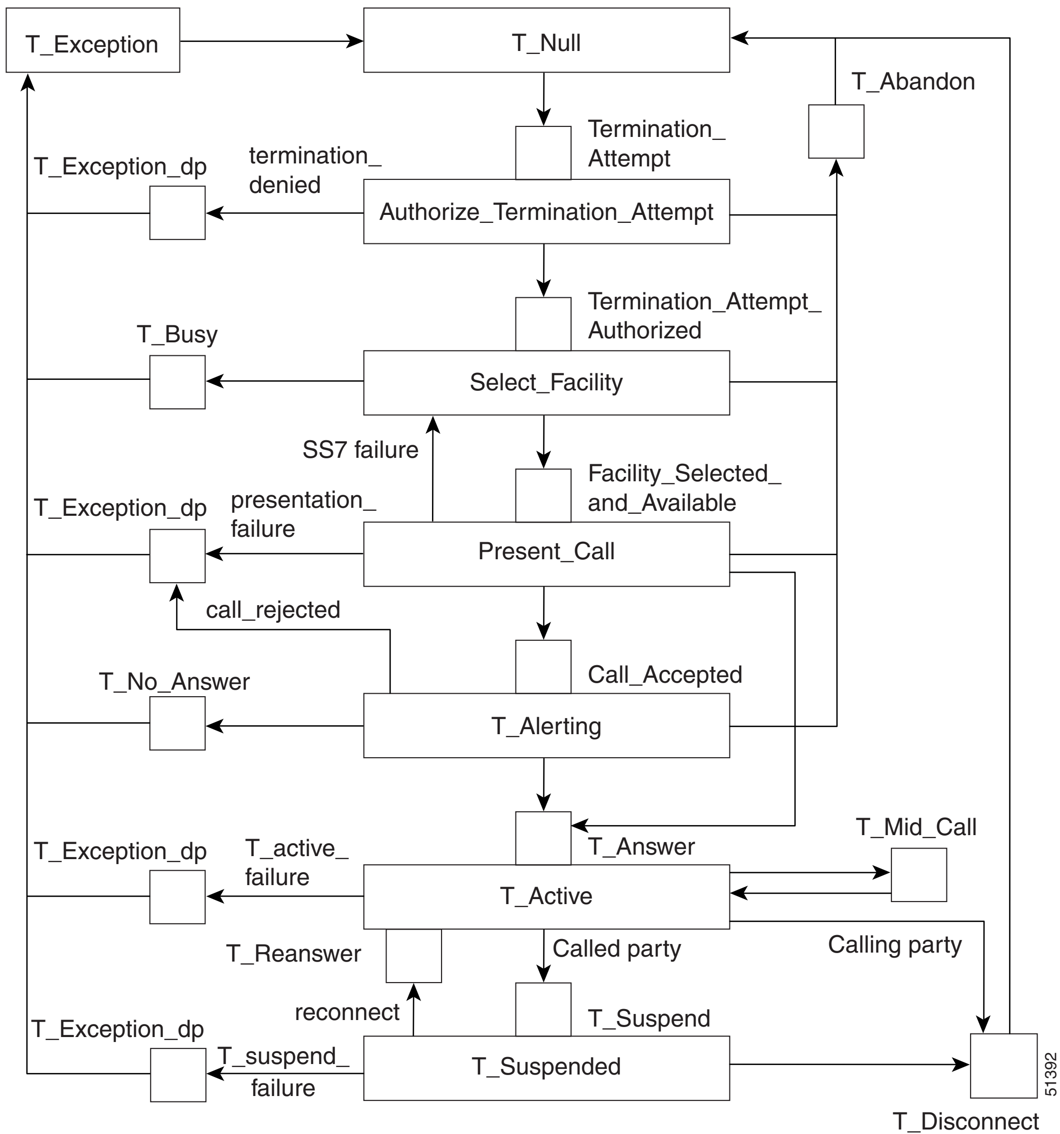


Table 6-1 lists the trigger detection points and trigger IDs for each feature.

Note Vertical service codes (VSCs) are assigned to some of these features. Refer to the Vertical Service Codes appendix of the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for VSC information.

Table 6-1 Features and Service Triggers

Feature	Description	Trigger Detection Point	Trigger ID
8XX	Toll free number	COLLECTED_INFORMATION	SPECIFIC_DIGIT_STRING
911	Emergency service	COLLECTED_INFORMATION	911_TRIGGER

Table 6-1 Features and Service Triggers (continued)

Feature	Description	Trigger Detection Point	Trigger ID
AC	Automatic callback (includes AC_ACT and AC_DEACT)		
AC_ACT	Automatic callback activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
AC_DEACT	Automatic callback deactivation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
ACR	Anonymous call rejection	TERMINATION_ATTEMPT_ AUTHORIZED	TERMINATION_ATTEMPT_ AUTHORIZED
ACR_ACT	ACR activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
ACR_DEACT	ACR deactivation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
ANI	Automatic number ID	No TDPs	No triggers
AR	Automatic recall (includes AR_ACT and AR_DEACT)		
AR_ACT	AR activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
AR_DEACT	AR deactivation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
BLV	Busy line verification	TERMINATION_ATTEMPT	BLV
CBLK	Call block (reject caller)	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CCW	Cancel call waiting	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CDP	Customize dial plan	COLLECTED_INFORMATION	CUSTOMIZE_DIALING_PLAN
CFB[1]	Call forwarding busy	T_BUSY	T_BUSY
CFBVA	CFB variable activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CFBVD	CFB variable deactivation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CFNA[1]	Call forwarding no answer	CALL_ACCEPTED	CALL_ACCEPTED
CFNAVA	CFNA variable activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CFNAVD	CFNA variable deactivation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CFU[1]	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[2]	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
CIDS	Delivery function of calling identity delivery and suppression	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CIDSS	Suppression function of calling identity delivery and suppression	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE

Table 6-1 Features and Service Triggers (continued)

Feature	Description	Trigger Detection Point	Trigger ID
CNAB	Calling name delivery blocking	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CNAM	Calling name delivery	FACITLITY_SELECTED_AND_AVAILABLE	TERMINATION_RESOURCE_AVAILABLE
CND	Calling number 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
COT	Customer originated trace	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
CPRK	Call park access code	O_MID_CALL	O_SWITCH_HOOK_FLASH_IMMEDIATE
		T_MID_CALL	T_SWITCH_HOOK_FLASH_IMMEDIATE
CPRK_RET	CPRK retrieval access code	No TDPs	No triggers
CT	Call transfer	O_MID_CALL	O_SWITCH_HOOK_FLASH_IMMEDIATE
		T_MID_CALL	T_SWITCH_HOOK_FLASH_IMMEDIATE
CW	Call waiting	T_BUSY	T_BUSY
DACWI	DACWI on DID calls	TERMINATION_ATTEMPT_AUTHORIZED	TERMINATION_ATTEMPT_AUTHORIZED
DND	Do not disturb	TERMINATION_ATTEMPT_AUTHORIZED	TERMINATION_ATTEMPT_AUTHORIZED
DND_ACT	Do not disturb activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
DND_DEACT	Do not disturb deactivation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
DPN	Directed call pickup without barge-in	No TDPs	No triggers
DPU	Directed call pickup with barge-in	No TDPs	No triggers
DRCW	Distinctive ringing call waiting	TERMINATION_ATTEMPT_AUTHORIZED	TERMINATION_ATTEMPT_AUTHORIZED
DRCW_ACT [3]	DRCW activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
		T_ANSWER	T_ANSWER
GSC1D	1-digit group speed call	COLLECTED_INFORMATION	SC1D_TRIGGER
GSC2D	2-digit group speed call	COLLECTED_INFORMATION	SC2D_TRIGGER
HOTLINE	Hotline feature	O_ATTEMPT_AUTHORIZED	O_ATTEMPT_AUTHD
ISFG	Incoming simulated facility group (SFG) for Centrex	TERMINATION_ATTEMPT_AUTHORIZED	TERMINATION_ATTEMPT_AUTHORIZED
LNP	Local number portability	COLLECTED_INFORMATION	LNP_TRIGGER

Table 6-1 Features and Service Triggers (continued)

Feature	Description	Trigger Detection Point	Trigger ID
MDN	Multiple directory numbers	TERMINATION_ATTEMPT_ AUTHORIZED	TERMINATION_ATTEMPT_ AUTHORIZED
OSFG	Outgoing SFG for Centrex	ROUTE_SELECTED	ROUTE_SELECTED
RACF [4]	Remote activation of call forwarding	T_ANSWER	T_ANSWER
RACF_PIN	RACF PIN change	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
		T_ANSWER	T_ANSWER
RCF	Remote call forwarding	TERMINATION_ATTEMPT_ AUTHORIZED	TERMINATION_ATTEMPT_ AUTHORIZED
REFER	REFER feature	O_MID_CALL T_MID_CALL	REFER_TRIGGER
SC1D	1-digit speed call	COLLECTED_INFORMATION	SC1D_TRIGGER
SC1D_ACT	1-digit speed call activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
SC2D	2-digit speed call	COLLECTED_INFORMATION	SC2D_TRIGGER
SC2D_ACT	2-digit speed call activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
SCA	Selective call acceptance	TERMINATION_ATTEMPT_ AUTHORIZED	TERMINATION_ATTEMPT_ AUTHORIZED
SCA_ACT [5]	SCA activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
		T_ANSWER	T_ANSWER
SCF	Selective call forwarding	TERMINATION_ATTEMPT_ AUTHORIZED	TERMINATION_ATTEMPT_ AUTHORIZED
SCF_ACT [6]	SCF activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
		T_ANSWER	T_ANSWER
SCR	Selective call rejection	TERMINATION_ATTEMPT_ AUTHORIZED	TERMINATION_ATTEMPT_ AUTHORIZED
SCR_ACT [7]	SCR activation	COLLECTED_INFORMATION	VERTICAL_SERVICE_CODE
		T_ANSWER	T_ANSWER
TWC	Three way call	O_MID_CALL	O_SWITCH_HOOK_FLASH_ IMMEDIATE
		T_MID_CALL	T_SWITCH_HOOK_FLASH_ IMMEDIATE
USTWC	Usage sensitive three way call	O_MID_CALL	O_SWITCH_HOOK_FLASH_ IMMEDIATE
		T_MID_CALL	T_SWITCH_HOOK_FLASH_ IMMEDIATE
WARMLINE	Warmline feature	O_ATTEMPT_AUTHORIZED	O_ATTEMPT_AUTHD

1. Multiple call forwarding is enabled by default, but can be disabled.
2. For Centrex users, an access code (typically provisioned as *52) can be used in conjunction with the CHD feature.
3. DRCW_ACT provides access to interactive voice response (IVR) server for activation, screening list setup and editing, and deactivation of DRCW.

4. RACF is an IVR-based function that can be used with CFU.
5. SCA_ACT provides access to IVR server for activation, screening list setup and editing, and deactivation of SCA.
6. SCF_ACT provides access to IVR server for activation, screening list setup and editing, and deactivation of SCF.
7. SCR_ACT provides access to IVR server for activation, screening list setup and editing, and deactivation of SCR.

Note The features DRCW_ACT, SCA_ACT, SCF_ACT, and SCR_ACT are collectively referred to as screening list editing (SLE) functions.

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 6-2), 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 Refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*, service-trigger table, for additional information about triggers for multiple features that are grouped into a service package.

Tip As shown in Figure 6-4 and Figure 6-5, 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 6-2 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
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

Table 6-2 Feature Precedence (continued)

No.	Trigger Detection Points (TDP)	Precedence
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.

Note 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.

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 6-3 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 6-3, 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 6-3 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 6-3 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 6-3 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 6-3 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	

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.

GLOSSARY

A

AAA authentication, authorization, and accounting

AC automatic callback

AC_ACT automatic callback activation

AC_DEACT automatic callback deactivation

ACR anonymous call rejection

ACR_ACT anonymous call rejection activation

ACR_DEACT anonymous call rejection deactivation

ACRA anonymous call rejection activation

ACRD anonymous call rejection deactivation

ADSL asymmetric digital subscriber line

AGW access gateway

AIN Advanced Intelligent Network

AIOD automatic identified outward dialing

ALI automatic location identification

AMA automated message accounting

ANC Announcements module

ANI automatic number identification

ANS announcement server

ANSI American National Standards Institute

API application programming interface

AR automatic recall

AR_ACT automatic recall activation

AR_DEACT automatic recall deactivation

AT	access tandem
ATA	analog telephone adaptor
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode

B

B-number	DN that a user enters as the forward-to number, also referred to as MN
BAF	Bellcore AMA format
BBG	basic business group
BCM	Basic Call module
BDMS	Bulk Data Management System
BEM	billing event message
BGDP	basic group dialing plan
BGL	business group line
BLA	billing adapter
BLV	Busy Line Verification
BP	block pair
BRIDS	Bellcore rating input database system
BS	billing server
BTA	basic trading area

C

CA	Call Agent
CAC	carrier access code
CALEA	Communications Assistance for Law Enforcement Act
CAMA	centralized automatic message accounting
CAS	channel-associated signaling
CAT	customer access treatment

CBLK	call block (reject caller)
CBR	constant bit rate
CCS	common channel signaling
CCW	cancel call waiting
CDB	call data block
CDP	custom dial plan
CDR	call detail record
CE	computing element
CFB	call forwarding on busy
CFBVA	call forwarding on busy variable activation
CFBVD	call forwarding on busy variable deactivation
CFNA	call forwarding on no answer
CFNAVA	call forwarding on no answer variable activation
CFNAVD	call forwarding on no answer variable deactivation
CFU	call forwarding unconditional
CFUA	call forwarding unconditional activation
CFUD	call forwarding unconditional deactivation
CFVBBG	call forwarding variable for basic business group
CFVABBG	CFVBBG activation
CFx	A general reference to all of the forwarding features (CFB, CFNA and CFU)
CHD	call hold
CIC	circuit identification code, carrier identification code
CID	calling identity delivery, also caller ID (see also CND)
CIDB	calling identity delivery blocking
CIDCW	calling identity delivery on call waiting
CIDS	calling identity delivery and suppression (per call)
CIDSD	calling identity delivery and suppression (per call)—delivery part
CIDSS	calling identity delivery and suppression (per call)—suppression part
CIP	carrier identification parameter

CLASS	custom local area signaling services
CLC	Carrier liaison committee
CLEC	competitive local exchange carrier
CLEI	common language equipment identifier
CLI	command-line interface
CLIP	calling line identification presentation
CLIR	calling line identification restriction
CLLI	Common Language Location Identifier
CMIP	Common Management Information Protocol
CMS	call management system
CMTS	Cable modem termination system
CNAB	calling name delivery blocking
CNAM	calling name delivery
CND	calling number delivery, calling number display
CNDB	calling number delivery blocking
CNM	connection module, customer network management
CO	central office
COCUS	central office code utilization survey
CODEC	coder/decoder, compression/decompression
COPS	Common Open Policy Service Protocol
CORBA	Common Object Request Broker Architecture
COS	class of service
COT	customer-originated trace, continuity testing, central office termination
CPCN	certificate of public convenience and necessity
CPE	customer premises equipment
CPRK	call park
CPRK_RET	call park retrieve
CPSG	call park subscriber group
CPU	call pickup, central processing unit

CS	Capability set (for example, CS-2)
CSA	Callpath services architecture
CSN	circuit switched network
CSR	Carrier sensitive routing
CT	call transfer, call type
CW	call waiting
CWI	call waiting indication

D

DA	directory assistance, distinctive alerting
DACWI	distinctive alerting call waiting indication
DPN	directed call pickup without barge-in
DPU	directed call pickup with barge-in
DF	delivery function (CALEA)
DID	direct inward dialing
DLEC	data local exchange carrier
DN	directory number
DND	do not disturb
DNIS	dialed number identification service
DNS	domain name server
DOD	direct outward dialing
DOW	day of week
DOY	day of year
DP	dial plan, dial pulse, demarcation point
DPN	directed call pickup without barge-in
DPN_O	directed call pickup without barge-in (originate)
DPN_T	directed call pickup without barge-in (terminate)
DPU	directed call pick-up with barge-in

DPU_O	directed call pickup with barge-in (originate)
DPU_T	directed call pickup with barge-in (terminate)
DRCW	distinctive ringing/call waiting
DRCW_ACT	distinctive ringing/call waiting activation
DPC	destination point code
DQoS	dynamic quality of service
DSL	digital subscriber line
DSP	digital signal processing
DSX	digital system cross-connect frame
DTMF	dual tone multifrequency

E

E-1	European equivalent of T1
E-911	Enhanced 911
E & M	“Ear and Mouth” switch-to-switch signaling on PSTN
EA	equal access
EC	echo cancellation
ECSA	Exchange Carriers Standards Association
EDP	event detection point
EM	event message
EMS	Element Management System, Event Messages Specification (PacketCable)
ERC	easily recognizable codes
ERQNT	Embedded Request for Notification
ESB	Emergency Service Bureau
ESL	emergency service line
ESP	encapsulating security payload
ETSI	European Telecommunications Standards Institute

F

FCAPS	fault, configuration, accounting, performance, security
FCI	furnish charging information
FCP	Feature Control Protocol
FGB	Feature group B
FGD	Feature group D
FIM	feature interaction manager
FS	Feature Server
FSAIN	Feature Server for Advanced Intelligent Network services
FSPTC	Feature server for POTS, Tandem, and Centrex services
FTP	File Transfer Protocol
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station

G

GAP	generic address parameter
GSM	global system for mobile communications
GUI	graphical user interface

H

HFC	hybrid fiber coax
HLR	home location register
HNPA	home numbering plan area
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol

I

IAD	integrated access device

IANA	Internet Assigned Numbers Authority
IAP	intercept access point
ICAP	Inter-call Agent Protocol
ICMP	Internet Control Message Protocol
IDDD	international direct distance dialing
IE	information element
IETF	Internet Engineering Task Force
IKE	Internet key exchange
ILEC	incumbent local exchange carrier
IMT	intermachine trunk
IN	intelligent network
INC	Industry Numbering Committee
IP	Internet Protocol
IPM	impulses per minute
IPsec	Internet Protocol security
IRDP	ICMP Router Discovery Protocol
ISA	ISDN adapter
ISDN	Integrated Services Digital Network
ISFG	Incoming simulated facility group
ISO	International Organization for Standardization
ISP	Internet service provider
ISS	ISDN stack
ISUP	ISDN user part
ITP	IP transfer point
ITU	International Telecommunications Union
IVR	interactive voice response
IXC	interexchange carrier

J

JCA	Java cryptography architecture, Java console agent
JCM	Java console module
JDBC	Java database connectivity
JMS	Java message service

K

KAM	keepalive module
Kbps	kilobits per second

L

LAN	local area network
LATA	local access and transport area
LCR	least cost routing
LDAP	Lightweight Directory Access Protocol
LEC	local exchange carrier
LERG	local exchange routing guide
LIDB	line information database
LNP	local number portability
LPC	local point code
LRN	local routing number
LRQ	location request (H.323 signaling)
LRU	least recently used
LSA	local serving area
LSSGR	LATA Switching Systems Generic Requirements

M

Mbps	megabits per second

MCF	multiple call forwarding
MCS	media gateway control stack
MDC	midcall
MDN	multiple directory numbers
MF	multifrequency
MG (MGW)	media gateway
MGA	media gateway adapter
MGC	media gateway controller
MGCP	Media Gateway Control Protocol
MGW (MG)	media gateway
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MLHG	multiline hunt group
MN	(See B-number)
MNM	maintenance module
ms	millisecond
MSA	Metropolitan Statistical Area
MSU	message signal units
MTA	Metropolitan Trading Area
MTP	Message transport part
MTU	maximum transmission unit
MWI	message waiting indicator

N

NANP	North American Numbering Plan
NAS	network access server
NCS	network-based call signaling
NE	network element

NEBS Network Equipment Building Standards

NFAS Non-Facility Associated Signaling

NIS Network information service

NMS network management system

NO network operator

NOC network operations center

NOD nature of dial

NPA Numbering Plan Area

NSE name signaling event

NTP Network Time Protocol

NU network unit

nxx NANP digits: n=2, 3, …9 and x=0, 1, …9

O

OAM operations, administration, and maintenance, Operations administration module

OAM&P operations, administration, maintenance, and provisioning

OCB outgoing call barring

OCN operating company number

OBCSM originating basic call state machine

OI operator interrupt

OLI originating line information

OMS OptiCall Messaging System

OPC originating point code

OPT Open Packet Telephony

OS operating system

OSA open service adapter

OSFG outgoing simulated facility group

OSI Open Systems Interconnection

OSS	operations support system
OSSGR	Operator Services Systems Generic Requirements

P

PBX	private branch exchange
PCM	pulse code modulation
PCMA	pulse code modulation A law
PCMU	pulse code modulation mu law
PCPS	Per-call presentation status
PCS	personal communications services
PCSNDB	personal communications services numbering database
PDU	power distribution unit
PIC	presubscribed interexchange carrier, Point in call
PLT	platform
POI	point of interface, point of interconnection
POP	point of presence
POPD	public office dialing plan
POSIX	Portable Operating System Interface UNIX
POTS	plain old telephone service
PPP	Point to Point Protocol
PPQ	point to point queuing
PPS	permanent presentation status
PRI	primary rate interface
PS	presentation status
PSAP	public safety answering point
PSTN	public switched telephone network
PVC	permanent virtual circuit

Q

QoS	quality of service

R

RACF	remote activation of call forwarding
RACF-PIN	remote activation of call forwarding personal ID number
RADIUS	remote authentication dial-in user service
RAID	redundant array of inexpensive disks
RAS	remote access server
	Registration, Admissions, and Status (signaling function in H.323 for communications to gatekeeper),
RCF	remote call forwarding
RDBS	routing database system
RDM	redundancy module
RDT	recall dial tone
RFC	Request for Comment (IETF)
RGW	residential gateway
RIP	Routing Information Protocol
ROH	receiver off hook
RPC	remote point code, remote procedure call
RQNT	request for notification
RR	resource record
RSA	rural service area
RSIP	restart in progress
RSM	resource module
RSVP	Resource Reservation Protocol
RTM	routing module
RTP	Real Time Transport Protocol
R-UDP	Reliable User Datagram Protocol (Cisco Systems proprietary signaling backhaul protocol)

S

S7A	SS7 adapter
S7S	SS7 stack (DGM&S)
SA	security association
SAC	service access calls
SAI	signaling adapter interface
SC1D	speed call 1-digit
SC1D_ACT	speed call 2-digit activation
SC2D	speed call 1-digit
SC2D_ACT	speed call 2-digit activation
SCA	selective call acceptance
SCA_ACT	selective call acceptance activation
SCF	selective call forwarding
SCF_ACT	selective call forwarding activation
SCP	service control point, signal control point
SCR	selective call rejection
SCR_ACT	selective call rejection activation
SDK	Software Development Kit
SDP	Session Description Protocol
SFG	simulated facility group
SFTP	Secure File Transfer Protocol (FTP)
SGCP	Simple Gateway Control Protocol
SIA	SIP adapter
SID	system identification number
SIM	service interaction manager
SIP	Session Initiation Protocol
SLE	screening list editing
SMA	SNMP adapter

SMDS	switched multimegabit data service
SMS	service management system
SNMP	Simple Network Management Protocol
SOHO	small office home office
SP	service provider
SPCS	stored program control system
SQL	Structured Query Language
SRST	Survivable Route Site Telephony
SS7	Signaling System 7
SSF	Service switching function
SSH	secure shell
SSL	secure sockets layer
SSP	service switching point, signal switching point
STP	signal transfer point
SVC	switched virtual circuit

T

T1	trunk level 1
T3	trunk level 3
TAP	Telocator Alphanumeric Paging Protocol
TBCSM	terminating basic call state machine
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Telecommunications device for the deaf
TDM	time-division multiplexing
TDP	trigger detection point
TF	toll free

TG	trunk group
TGW	trunking gateway
TMN	Telecommunications Management Network
TNS	transit network selection
TOD	time of day
TOPS	traffic operator position system
TOS	type of service
TPM	terminating point master
TRS	telecommunications relay services
TSAP	transport service access point
TTY	text typewriter
TWC	three-way calling

U

UAA	user authentication adapter
UAC	user agent client
UAS	user agent server
UBR	universal broadband router (Cisco)
UCD	uniform call distribution
UDP	User Datagram Protocol
URI	uniform resource identifier
URL	universal resource locator
USTWC	usage-sensitive three-way calling

V

VBR	variable bit rate
VLAN	virtual LAN
VMWI	visual message waiting indicator

VoATM	voice over ATM
VoIP	voice over IP
VSC	vertical service code

W

WAN	wide area network
WFI	waiting for instruction

X

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

Y

Z


INDEX

M

N

O

P

R

S

T

W