Cisco BTS 10200 Softswitch System Description, Release 7.0

July 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-23035-01

Cisco BTS 10200 Softswitch System Description, Release 7.0

CONTENTS

Preface

Revised: July 2010, OL-23035-01

This document provides an overview of the components, functions and signaling protocols supported by 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"

This document also includes the Glossary and Index.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Document Change History

The following table lists the revision history for the *Cisco BTS 10200 Softswitch System Description, Release 7.0*.

Version Number	Issue Date	Status	Reason for Change
OL-23035-01	July 2010	Initial	Initial document for Release 7.0.

CHAPTER 1

Cisco BTS 10200 Softswitch Technical Overview

Revised: July 2010, OL-23035-01

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

Tip The companions to this document are the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions Guide* [contains descriptions of network features, subscriber features, class of service (CoS) functions, outgoing call barring (OCB), feature interactions, and interactive voice response (IVR) features] and the *Cisco BTS 10200 Softswitch Site Preparation and Network Communications Requirements* (contains information on site preparation and network communications requirements).

Introduction

The BTS 10200 is a software-based, class-independent network switch. It provides call-control intelligence for establishing, maintaining, routing, and terminating voice calls on media gateways (MGWs) in the packet network, 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 BTS 10200 provides the major signaling functions performed by traditional Class 4 and Class 5 switching systems in the PSTN. It also provides more than 60 provisionable subscriber features, and management interfaces for provisioning, monitoring, control, and billing operations.

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

When BTS 10200 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 BTS 10200. 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 BTS 10200 communicates with a wide range of network elements (NEs) including:

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

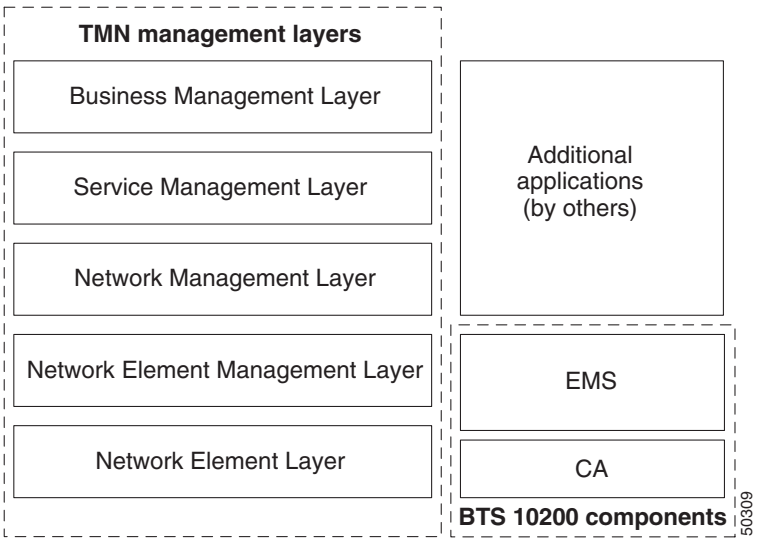
When you order the BTS 10200 software, your Cisco account team will work with you to determine appropriate hardware options, software loads, and database sizing options for each of your sites.

Note The selected database sizing option is set when the BTS 10200 software is installed on your system. Details of the software installation are provided in the *BTS 10200 Application Installation Procedure*.

The BTS 10200 in the TMN Model

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

Figure 1-1 BTS 10200 Components in the TMN Model



Note The Call Agent (CA) and Element Management System (EMS) components of the BTS 10200 shown in Figure 1-1 are described in the "Logical Components" section on page 1-11.

The role of each TMN layer is described below.

Business Management Layer roles:

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

Service Management Layer roles:

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

Network Management Layer roles:

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

Network Element Management Layer roles:

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

Network Element Layer roles:

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

Interoperability

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

Caution Some features involve the use of other network NEs deployed in the service provider network, for example, gateways, media servers, announcement servers, embedded multimedia terminal adapters (eMTAs), and Session Initiation Protocol (SIP) phones. See the "Component Interoperability" section of the *Cisco BTS 10200 Softswitch Release Notes* for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the BTS 10200 Release 7.0 software. Earlier or later releases of platform software might be interoperable with the BTS 10200 and it might be possible to use other functions on these platforms. The list in the *Release Notes* certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the BTS 10200.

Overview of Features and Functions

The BTS 10200 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, page 1-4
- Subscriber Features and Functions, page 1-7
- Billing Features and Functions, page 1-8
- Operations, Maintenance, and Troubleshooting Features and Functions, page 1-8
- Provisioning Features and Functions, page 1-10
- System Administration Features and Functions, page 1-10

Note 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 on MGWs in the packet network, while seamlessly operating with circuit-switched networks.
- Support for a number of network signaling protocols, including Media Gateway Control Protocol (MGCP), SIGTRAN for Signaling System 7 (SS7), H.323, PacketCable, 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 by command-line provisioning:
  - Trunk-based routing, with three trunk group (TG) selection options: 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 several types of trunk testing, including T108, 911 Feature Group D Operator Support (FGD-OS), 911 Feature Group D, and loopback testing for NCS/MGCP subscriber endpoints.
- Support for route advance—The route table in the BTS 10200 database allows the service provider to provision a list of up to 10 trunk groups (TG1 to TG10), and includes a parameter for selecting the priority of the TGs for routing (TG-SELECTION). The system attempts to route each 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 three times. (Any TG in the list that is administratively out of service is not counted as an attempt.) If all three attempts fail, the call is released, and the system provides a release announcement.
- Digit manipulation function, which enables the BTS 10200 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 based on ANI (automatic number identification), and the called party number is based on 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 ANSI and ITU local number portability (LNP) procedures.
- 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 (BTS 10200) 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.

- Support for several national ISUP versions.
- Support for ISDN User Part (ISUP) transparency with the Cisco PGW 2200.
- Interoperability with PBX equipment through the ISDN-PRI and CAS protocols.
- Generation of triggers, allowing 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, which 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 through the 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), 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.
- An auditing and reporting function that provides data consistent with the North American Numbering Plan Administration (NANPA) audit requirements for primary and intermediate carriers. The NANPA audit report provides information on telephone-number data that is provisioned in the BTS 10200.
- Alerting notification to a third-party feature server. The service provider can use appropriately designed and configured feature servers to make use of this notification and data to provide value-added services to subscribers; for example, delivery of caller ID on a subscriber television or computer screen.
- SIP triggers (provided for MGCP, Network-Based Call Signaling (NCS), and SIP subscribers). The SIP Triggers feature uses the SIP protocol, with some extensions, to enable the BTS 10200 to interoperate with third-party application servers so that Multi-Service Operators (MSOs) can provide customers with enhanced features and services. The triggers can be used by the third-party servers to provide both originating services (such as TV caller ID, custom ringback, and voice dial), and enhanced terminating services.
- Call Agent controlled mode for RFC 2833 DTMF Relay. During call setup, the CA (the BTS 10200) can authorize an eMTA or media gateway (MGW) to invoke RFC 2833 DTMF relay procedures.
- Support for PacketCable Multimedia (PCMM)-based QoS for type 1 clients. Type 1 clients refers to endpoints using SIP, MGCP, or H.323 as the call signaling protocol. (The system supports this PCMM-based feature in addition to all of the PacketCable-based features provided in earlier releases.)

- Emergency 911 overflow announcement. The system plays an announcement when all circuits to the emergency center are busy and the emergency call cannot be completed to the emergency center. This feature requires the announcement resource to be available and applicable.
- Emergency 911 trunk connection loss alarm. The BTS 10200 is capable of generating a critical alarm of when an emergency trunk resource becomes remotely or locally blocked.
- Display of the number of currently active emergency calls. The query call-count command displays all emergency calls currently active on the BTS 10200. With this command, you specify the call type that you want included in the count: emergency, police, ambulance, fire, all-emergency, or all.
- Emergency callback (ECB)—This feature allows a public safety answering point (PSAP) operator to call back a subscriber provisioned on the BTS 10200. The BTS 10200 treats these callbacks as special high-priority calls, and all terminating features that could potentially interrupt a call from a PSAP operator are disabled. ECB is an office-based feature; the system can provide ECB treatment to any subscriber associated with an office service that is provisioned with ECB.
- Hostage negotiation feature—This feature allows you to provision a BTS 10200 subscriber for hostage negotiation calls. The feature restricts incoming calls to and outgoing calls from the subscriber hostage. Regardless of the directory number (DN) the hostage subscriber dials, the outgoing call terminates at HOSTAGE_OUTBOUND_DN, which connects the hostage subscriber directly to the law enforcement authority (LEA).
- Telephony Application Server (TAS) feature—The Telephony Application Server (TAS) TAS application allows the BTS 10200 to communicate with serving call session control function (S-CSCF) servers over an IP multimedia service control (ISC) interface to provide subscriber calling features. The TAS can perform origination processing and termination processing; it can also route calls if requested by the originating S-CSCF. The TAS and the S-CSCF are both SIP-based applications. (The S-CSCF is external to the BTS 10200.)
- Support for Sh Interface between the Cisco BTS 10200 Softswitch acting as a Telephony Application Server (TAS) and a Home Subscriber Server (HSS).

Note See Chapter 1, "Network Features," in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions Guide* for complete coverage.

Subscriber Features and Functions

The system supports the following subscriber features and functions:

- 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, privacy screening, and caller identification. See the *Subscriber Features" chapter in the Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions Guide* for complete coverage.
- Class of service (CoS) screening and outgoing call barring (OCB). See the *Class of Service and Outgoing Call Barring Features"* chapter in the *CIsco BTS 10200 Softswitch Network and Subscriber Feature Descriptions Guide* for complete coverage.
- Limited call duration (LCD) service, including support for both prepaid (debit) and postpaid (credit) services.

- Temporarily disconnected subscriber status, including provisionable restrictions on incoming and outgoing calls.
- Call Pickup feature for centrex subscribers.
- Enhanced interaction between CHD and CW features for centrex subscribers.
- Enhanced MLHG feature—allows the service provider to route a call, from an idle terminal that does not answer a call to the next available terminal. The routing is based on the timer value set (in seconds) in the MLHG table. The feature also allows to rollover the call to voicemail—if the voicemail service is configured for the number. The voicemail rollover occurs when all the hunted terminals are busy or idle, and the last terminal of the hunted line is reached.

Note See the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions Guide, Release 7.0* for detailed description of these features.

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
- Configurable option to use either a native file-naming convention or a PacketCable EM convention for CDB file names
- Option to designate billing as either flat rate or measured rate for individual subscribers
- Support for long-duration-call information in the billing record
- Metered billing with collection of metered “pulses” from operators signaled through SPIROU (French ISUP) ITX messages
- Enhancement to identify business digital voice subscribers in the billing record.

Note See the *Cisco BTS 10200 Softswitch Billing Interface Guide, Release 7.0* 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 becomes corrupted. In such a case, the data must be restored from a backup file.

- Heap monitor—The system periodically monitors heap usage of all the processes started by a platform and issues an alarm when the heap usage of a process goes beyond a predefined threshold level.
- 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 BTS 10200 is in a congested state, emergency messages are given special treatment and are allowed to pass through.
- Log archive file (LAF)—Transports trace log files to a remote archive server for storage. LAF is a continuously running daemon process on all nodes (components) of the BTS 10200. It wakes up every minute when active and checks if there are any new log files. The service provider can specify the external archive system, the target directory, and the disk quota for each trace log directory in the system. If any new log files are in these trace log directories, LAF transfers them by Secure FTP (sftp) to an external archive server specified by the service provider.
- Automatic shared memory backup (ASMB)—Provides the ability to create a backup copy of the Call Agent/Feature Server (CA/FS) shared memory database, which helps the operator restore a CA/FS system in the event of disaster. The restoration procedure should be run only if the shared memory is corrupted in both the active and standby sides of the network element.
- Automatic restart function—Attempts to automatically restart OOS-FAULTY platforms into a STANDBY state.

  It can also:
  - Initiate a platform switchover if a process experiences multiple restarts.
  - Automatically save useful debugging information if a platform shutdown occurs.
- Internal Secondary Authoritative DNS Server (ISADS)—A local DNS database that runs on BTS 10200 host machines and shadows the primary DNS server in the service provider network. If the primary DNS server has a long outage, the ISADS can respond to DNS queries by the BTS 10200 applications.

- Fast-audit and synchronization tools—Scripts that can be run on the root level of the host machines to perform database audits on the network elements of the system and synchronize any mismatches between network elements.
- BTSSTAT software utility—Displays the operational status of all components of the BTS 10200 system.
- Call tracer (CTRAC) feature—A mechanism that marks each call with a unique ID. This allows the operator to use a UNIX grep or a similar command to filter out the lines of interest during a troubleshooting effort.
- Native data export—This feature allows you to export all provisioning data from the BTS 10200 by the use of a command line interface (CLI) command. Execution of the CLI command stores the exported data in a user-named output file in text format in the export directory.

Note See the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide* or the *Cisco BTS 10200 Softswitch Troubleshooting Guide* for specific operating and maintenance procedures.

Provisioning Features and Functions

The system supports the following provisioning features and functions:

- A provisionable database containing data for basic call processing, billing, and special call features.
- Command autocompletion and context-sensitive help.
- The synchronous provisioning feature provides a provisionable option that directs the system to wait for all provisioning commands to be executed before a control or status command is executed. The system also provides a CLI command that retrieves detailed information about pending transactions.
- Common Object Request Broker Architecture (CORBA) Adapter (CAD) interface—The CAD provides an abstraction of the BTS 10200 in a consistent, object-oriented model. The CAD interface supports a means of provisioning the BTS 10200 that parallels the CLI adapter capabilities. The system provides a secure socket layer (SSL) transport for the CORBA adapter. For CORBA details, see the *Cisco BTS 10200 Softswitch CORBA Adapter Interface Specification Programmer's Guide*.
- Support for Call Management Server (CMS) subscriber provisioning through a Simple Object Access Protocol (SOAP)/XML interface. The SOAP interface is compliant to a subset of the PacketCable 1.5 CMS provisioning specification, PKT-SP-CMSPROV1.5-I01-050128, and provides a SOAP communication layer for the acceptance and translation of specific BTS 10200 XML requests.
- Support for an external Feature Interaction Module/Extensible Markup Language (FIM/XML) file that allows you to define the interaction between external and internal features. (External features are those provided by servers outside the BTS 10200 and internal features are those provided by the BTS 10200.) Each BTS 10200 release includes an original FIM/XML file. The offline FIM/XML tool, provided with the file, allows you to define a new external feature or modify existing interactions involving existing features.

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 BTS 10200 runs on Sun Solaris. Processes and utilities in the UNIX system that are unsuitable for use in a softswitch environment have been disabled.
- Communication with the existing Operations Support System (OSS) infrastructure—including network management systems (NMSs)—to support fault, configuration, accounting, performance, and security (FCAPS) functions.

Logical Components

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

List of Logical Components

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

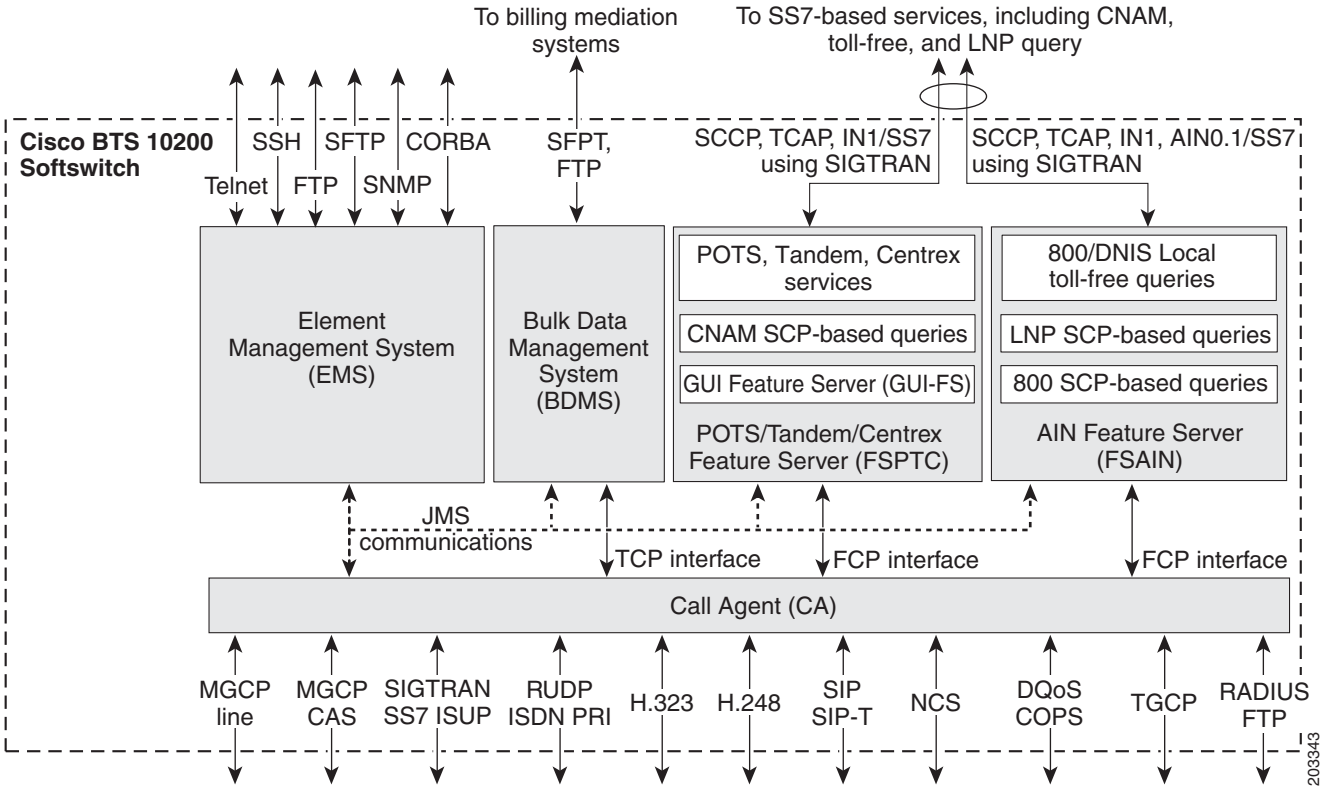
- Call Agent (CA)—Serves as a call management system and media gateway controller. It handles the establishment, processing, and teardown of telephony calls.
- Feature Servers (FSs)—Provide plain old telephone service (POTS), Tandem, Centrex, and Advanced Intelligent Network (AIN) services to the calls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

  There are two types of FSs in the BTS 10200:

  - FSPTC—FS for POTS, Tandem, and Centrex features
  - FSAIN—FS for AIN services
- Element Management System (EMS)—Controls the entire BTS 10200 and acts as a mediation device between an NMS and one or more CAs. It is also the interface for the provisioning, administration, and reporting features of the BTS 10200.
- 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.
- Internal Secondary Authoritative DNS Server (ISADS)—The ISADS provides an internal DNS database identical to the DNS database in the network. This internal DNS server can respond directly to DNS queries if necessary.

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

Figure 1-2 BTS 10200 Architecture, Showing Logical Components



CA Functions

The Call Agent (CA) provides monitoring and control of external NEs. It connects to multiple networks through the signaling adapter interface. This interface converts incoming and outgoing signaling (which is based on industry signaling standards) to and from the 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

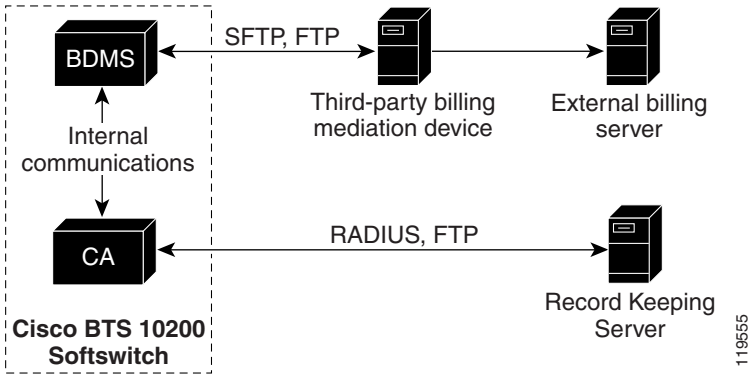
- Provide maintenance primitives for signaling link hardware maintenance and signaling protocol stack provisioning

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 in internal communications to the BDMS (see Figure 1-3). The BDMS forwards this data by 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 1-16.
- 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 We strongly recommend that you 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 BTS 10200.

For additional descriptions and provisioning procedures applicable to CDB-based billing, see the *Cisco BTS 10200 Softswitch Billing Interface Guide*. For EM-based descriptions and provisioning procedures, see the *Cisco BTS 10200 Softswitch PacketCable Guide*.

FS Functions

There are two different types of FSs in the BTS 10200.

- FSPTC—FS for POTS, Tandem, and Centrex features

- FSAIN—FS for Advanced Intelligent Network services

Each FS communicates internally with the CA and externally (through a signaling gateway) with signal transfer points (STPs) that are part of the SS7 signaling system.

The FSs provide access to features through a well defined interface. The BTS 10200 architecture logically separates the FSs (which provide feature control) from the CA (which provides call control). This architecture also defines a clear interface, Feature Control Protocol (FCP), between the FSs and the CA. 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 BTS 10200 call processing mechanisms are based on the ITU CS-2 call model. For details on the call model and triggers, see the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions Guide*.

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 BTS 10200 adjusts its query rate accordingly.

EMS Functions

The EMS) manages all of the BTS 10200 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 over 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 through Oracle in the EMS/BDMS and through an indexed database (IDX) in the CA/FS.

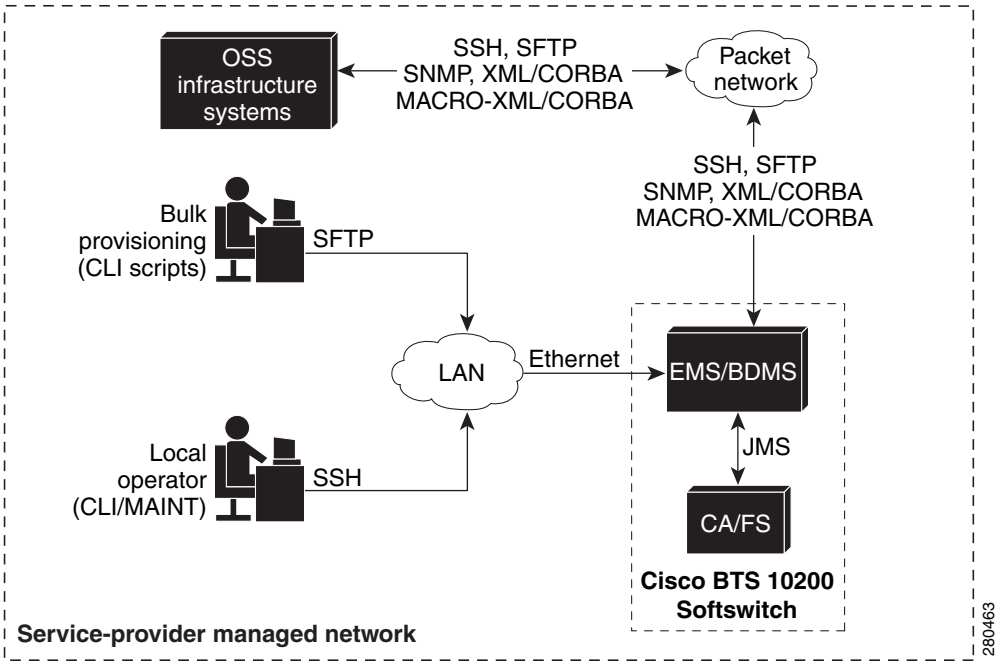
Note For additional information on using these functions, see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide,* the *Cisco BTS 10200 Softswitch Provisioning Guide*, and the Cisco BTS 10200 Softswitch CLI Database.

The EMS provides a flexible mechanism for transporting information over any protocol to any external device. The EMS interface design takes into account that each carrier has its own unique set of OSSs. The EMS provides a decoupling layer between the external protocols used within the service provider network and the internal protocols of the BTS 10200. 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 EMS Management Interfaces for Service Provider



The user interfaces include the following:

- Secure shell (SSH)—For provisioning in the CLI and Maintenance (MAINT) shells.
  - CLI shell—User interface for entering commands and their parameters in command-line format. The user must log in to the active EMS. The session terminates if it is idle for a provisionable number of minutes (see the idle-time parameter in the session table, default = 30 minutes) or if there is an EMS switchover from active to standby. This shell displays the CLI> prompt.
  - MAINT shell—Provides a maintenance interface for CLI commands that does not time out or disconnect on switchover. This shell can be used, if necessary, for maintenance and recovery purposes. The MAINT user can log in to either the active or standby EMS. This interface supplies a prompt based on the username, rather than a CLI> prompt.

Caution The MAINT shell is not intended for normal provisioning activities. We strongly recommend that you use it only if the CLI shell is unusable in a maintenance or recovery scenario. An unattended MAINT session does not autodisconnect.

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

Note For security purposes, Telnet is not supported.

- XML/CORBA and MACRO-XML/CORBA support the following:
  - CORBA provisioning and monitoring interface

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 BTS 10200
- Simple Network Management Protocol (SNMP)—Provides traps, status, control, and measurement functions, and provisionable community strings.

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

Note The functions of the BDMS component, including billing-related communications links, are described in the "BDMS Functions" section on page 1-16.

SNMP Agent

The following functions are supported by the BTS 10200 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 in turn imports three other MIBs—IPCELL-TC, SNMPv2-TC, and SNMPv2-SMI. The main MIB uses variables from these other three MIBs.

BDMS Functions

The 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 on page 1-17). 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 BTS 10200 to adapt to changes in the billing mediation device interface. The BDMS transmits billing records by FTP or SFTP to the mediation device at regular time intervals that are provisionable in the BTS 10200.

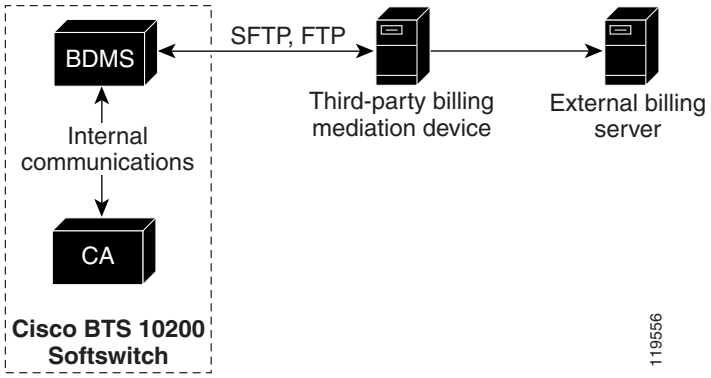
The BDMS provides the following billing functions:

- Supports batch record transmission using 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 by 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 BTS 10200.

Figure 1-5 Billing Interface to the BDMS



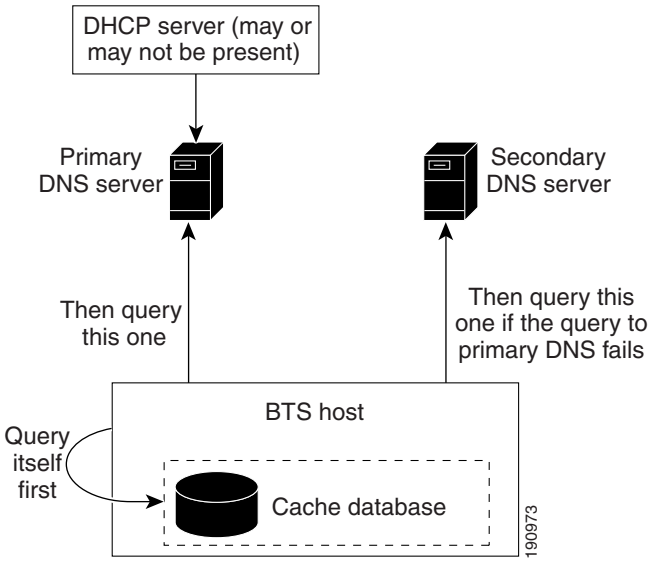
Internal Secondary Authoritative DNS Server (ISADS)

The internal secondary authoritative DNS server (ISADS) provides the BTS 10200 with an internal DNS database identical to the DNS database in the network. All the domain name queries from the BTS 10200 go first to this internal server. If there is a long DNS outage in the network, a prolonged network outage, or a failure of an external DNS server, the internal DNS server can respond to DNS queries, and the BTS 10200 can still perform its usual functions with less risk of interruption.

Feature Description

In the “cache database” design, if a user chooses to set up a named process, it acts only as a cache server. All the DNS queries, except those in its cache, are forwarded to other DNS servers (in this case, the primary DNS server and/or secondary DNS server). Even those responses from the cache are not authoritative. Therefore there is still a heavy dependence on the primary/secondary DNS servers in the network. If there is a long DNS outage, the data in the cache eventually expires. BTS 10200 applications that issue queries to the DNS server get no response, or a slow response. This can cause applications to block for longer intervals. See Figure 1-6.

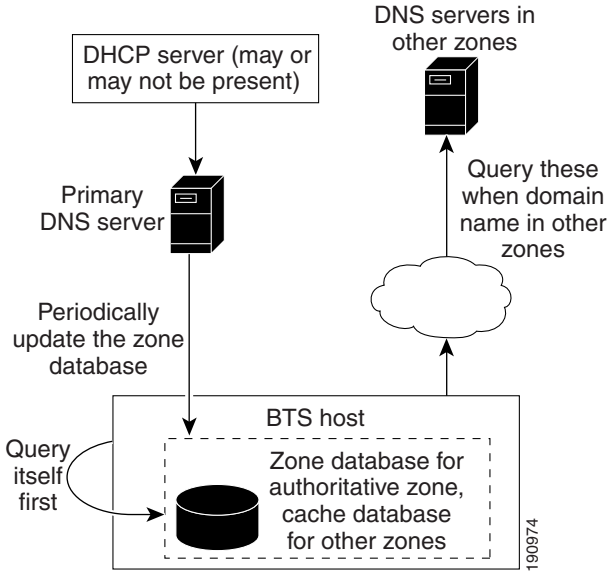
Figure 1-6 Design with Internal Secondary Cache-Only DNS Server



With the ISADS-based design, an ISADS can be directly configured and installed on every node of a BTS 10200 system or just on the CA. The ISADS in the BTS 10200 system periodically gets the database update from the primary DNS server. The ISADS basically mirrors the primary DNS server's database.

When a BTS 10200 application issues a query, it first queries the ISADS. This ISADS responds directly, without contacting the outside primary DNS server. If there is a long primary DNS server outage in the network, the BTS 10200 applications can always get an authoritative response. However, this internal DNS database can become outdated as time goes by. See Figure 1-7.

Figure 1-7 Design with ISADS



Restrictions and Limitations

The primary DNS server (which might not be a Cisco product) must support incremental zone transfer (IXFR) and dynamic update on the primary DNS server. If Berkeley Internet Name Daemon (BIND) is used as the primary, do not use a version of BIND older than Version 9. Check the manual or consult with the vendor that supplies the DNS program for your primary DNS server to verify that BIND Version 9 or later is being used. CNR Release 6.X also supports BIND.

Industry Standards

The ISADS capability is based on the following industry standards.

Standard	Title
RFC 1034	Domain Names—Concepts and Facilities
RFC 1035	Domain Names—Implementation and Specification
RFC 1995	Incremental Zone Transfer in DNS

Installing

You must configure the primary DNS server and the BTS 10200 hosts (where ISADS will be located). Set up the configuration file manually before the fresh installation. For details on how to set up the configuration files, refer to Appendix G, *Application Installation Procedure*. For information on how to configure existing systems, refer to Appendix H, *Application Installation Procedure*.

The installation will have a new parameter for the BTS 10200 ISADS feature. In the opticall.cfg file (the customer configuration file), the parameter "NAMED_ENABLED" will be preserved to indicate whether or not the user wants to start up a named process.

NAMED_ENABLED has the following four possible values:

- n: Do not start up the named process.
- cache_only: Start up the named process as cache server only.
- secondary_dns_all_hosts: Start up the named process as an ISADS in all BTS 10200 hosts in this system.
- secondary_dns_CA_only: Start up the named process as an ISADS in CA hosts only.

Set up the configuration file manually before the fresh installation/upgrade. The installation/upgrade should be done in a nonpeak hour, because the first download of the database from the primary DNS server to the ISADS servers might be time consuming.

Configuring

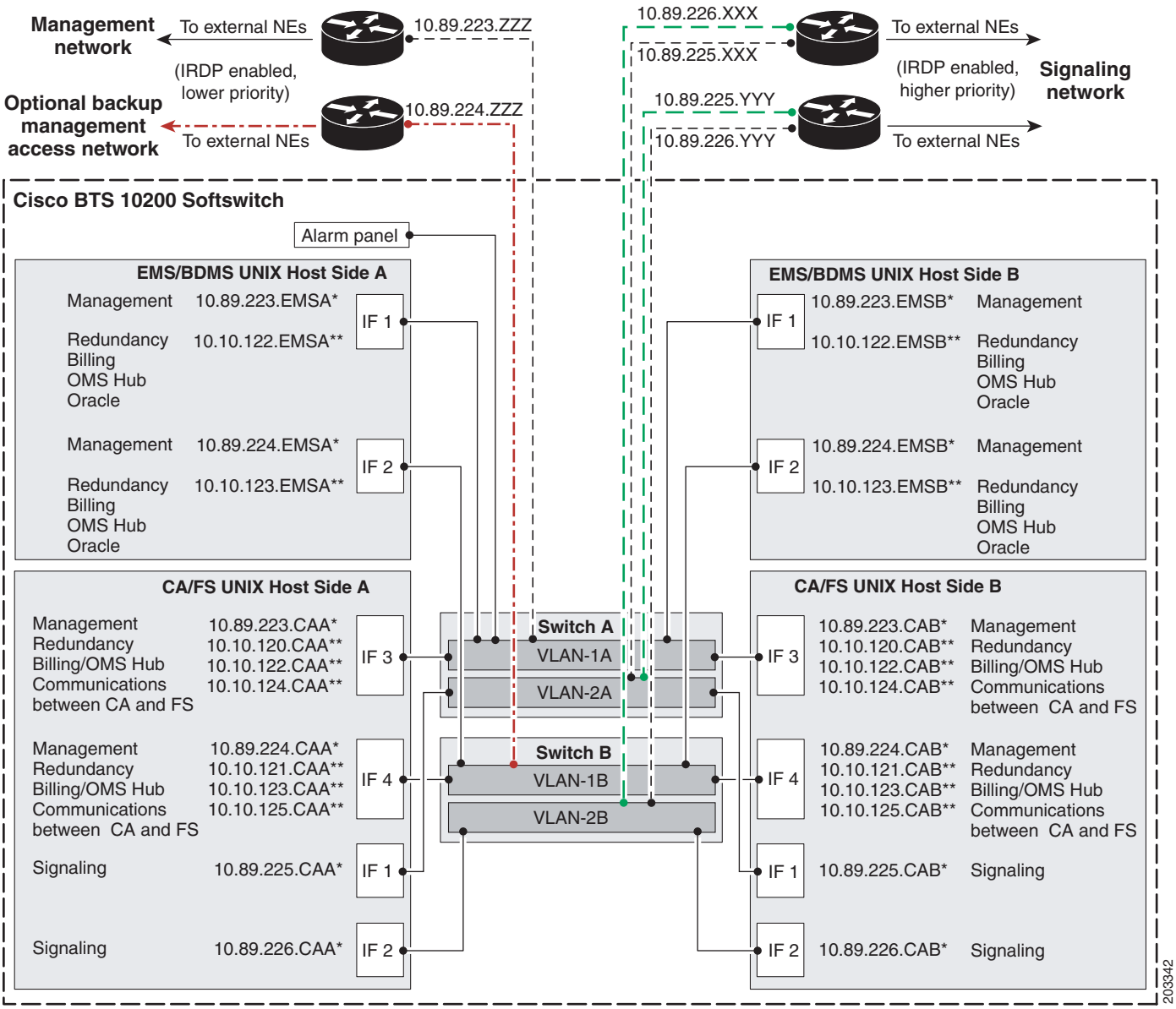
To configure the primary DNS server, refer to Appendix G, *Application Installation Procedure*.

To configure the internal secondary DNS server, refer to *Appendix G, Application Installation Procedure*.

Reliability and Availability of Components

The BTS 10200 network configuration is shown in Figure 1-8. This configuration provides redundant host machines for the EMS/BDMS and CA/FS components, redundant management of 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.

Figure 1-8 BTS 10200 Network Configuration



Notes for Figure 1-8

1. The following labels represent specific components and functions:
   - IF = Interface. The numbers for IF1, IF2, IF3, and IF4 match the order of appearance in the ifconfig process.
   - 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 transferred 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 BTS 10200 is in the *Network Information Data Sheet (NIDS)* 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 priority lower 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 (by SSH, SFTP, and so forth), DNS services, and outbound billing data by FTP or SFTP
   - Uplinks for external communications, used for connection to external NEs over an IRDP-enabled network
5. To access the management network of the BTS 10200 from an external host, we recommend that you deploy the external host on the same network as the CA management networks. If you prefer to deploy the external host on a different network, you must set up a static route on each of the CA hosts, and this allows for administrative access to the CAs from other networks.
6. To support full system redundancy, you must connect the external uplinks from the Catalyst switches to separate routers, as shown in Figure 1-8:
   - 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. We recommend that two (redundant) DNS units be deployed in the service provider network, and that the two DNS units be reachable over separate networks with diverse routing paths. We also recommend that you place the DNSs behind a load balancer so that a single IP address is exported to clients such as the BTS 10200.

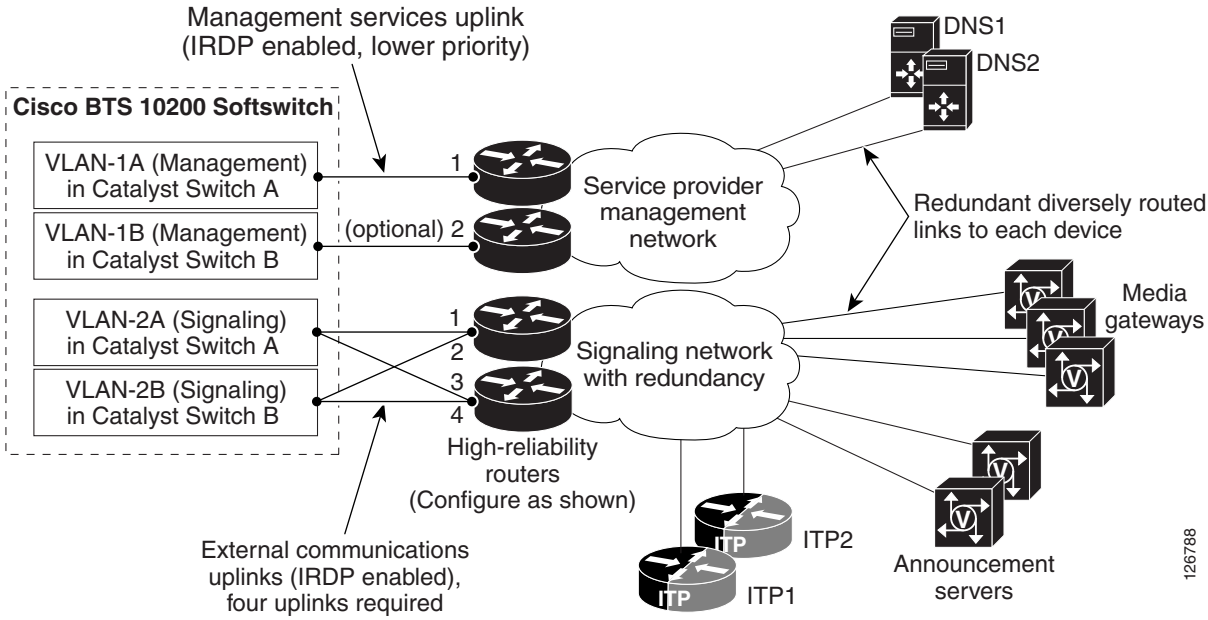
Note The system provides additional support for DNS availability through the internal DNS functionality. See the "Internal Secondary Authoritative DNS Server (ISADS)" section on page 1-17.

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

Figure 1-9 shows an example of communication paths between the BTS 10200 and NEs in the managed network. The initial software configuration of the BTS 10200 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 1-9 Uplinks and Communications Paths to NEs in the Managed Network



Notes for Figure 1-9

1. IRDP on the management network routers must be set at a priority lower than the IRDP level on the signaling network.
2. The uplinks are used as follows:
   - Two uplinks for management services (through connection modes such as SSH and SFTP), DNS services, and outbound billing (through FTP and SFTP)

- Four uplinks for external communications for VoIP signaling based on protocols such as MGCP, SIP, H.323, COPS, and SIGTRAN

Note The four signaling uplinks must be connected to the appropriate internal VLANs of the BTS 10200, as shown in Figure 1-9.

3. See also the additional notes provided with Figure 1-8.

Dual Active/Standby 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 highlight any corruption. The audit reports any data structure inconsistencies or corruption by providing 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 calls being lost. 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, and 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 transfers the IP addresses of the logical interfaces over to the newly active CA/FS side.

  Note IP Manager transfers IP addresses only if they are on the same subnet. In the case of a multihomed platform, when one of the interfaces fails, IP Manager does not transfer 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 BTS 10200 process exits because of 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 switches over to the mate.

Automatic Restart Function

The automatic restart function performs as follows:

- If a platform (EMS/FS/CA) transitions to OOS-FAULTY, the system automatically saves data useful for offline debugging (trace logs, status files, cores, and so forth). In many cases the system then automatically attempts to restart the platform to the STANDBY state. The automatic restart is intended to reduce the risk of outages by reducing the amount of time the system is in simplex mode.
- If a process exceeds the maximum number of restarts, the system initiates a switchover of the affected platform. A switchover is more efficient than allowing the platform to transition to the OOS-FAULTY state, which requires the standby side to go through the taxing database copy process. However, the system does not automatically save debugging data during this switchover.

For more detailed information on this process, see the "Automatic Restart" section in the *Cisco BTS 10200 Softswitch Troubleshooting Guide*.

Asynchronous DNS Lookup Function

The asynchronous DNS lookup feature allows the BTS 10200 to continue call processing for MGCP-based calls while it is performing a DNS lookup. (Synchronous lookup means that call processing is delayed until the DNS lookup is complete; asynchronous lookup means that call processing continues without waiting for the completion of the lookup.) This feature makes the BTS 10200 robust in case of DNS server failures.

If the DNS server(s) fail or exhibit poor response times, synchronous DNS function calls could seriously impact call processing by throttling new calls and failing existing calls. Very slow DNS responses from improperly provisioned media gateway (MGW) fully qualified domain names (FQDNs) or slower responses from any MGW FQDNs that are not provisioned in the DNS server seriously impact existing call processing. Even call processing for MGWs that have very fast DNS responses can be impacted.

The scope of this feature is limited to the MGCP interface only. The supported protocols include all gateway control protocols (xGCP), including PacketCable NCS and TGCP.

The BTS 10200 launches asynchronous DNS lookups to resolve FQDNs of the MGWs while attempting to send MGCP messages. It also makes the resolved IP addresses for FQDNs available to the standby side of the BTS 10200 for instant use without launching new DNS queries. When a BTS 10200 is started or restarted, it starts using the IP address in the BTS 10200 internal MGW DNS cache if available, and also triggers reconfirmation of that IP address from the DNS server.

The applicable parameters for this feature are src-addr-change-action and domain-name-caching-supp in the Media Gateway Profile (mgw-profile) table. There is also one provisionable timing parameter, max-num-of-dns-lookups in the Call Agent Configuration (ca-config) table. The operator can provision these parameters to accept or reject and confirm or ignore the IP address of any FQDN and update the

IP address if it is different. When an MGW reboots, the BTS 10200 (if provisioned with the default setting, src-addr-change-action=confirm) reconfirms its IP address from a DNS server and updates it in the BTS 10200 internal MGW DNS cache if the IP address there is different.

Cisco Specified Hardware

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

General Hardware Description

Each newly installed BTS 10200 requires the following hardware. See the *Cisco BTS 10200 Softswitch Release Notes* for information regarding specific hardware models and Solaris patch levels.

- Four UNIX-based host machines running the Solaris operating system.
- Two Cisco Catalyst 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.

Important Notices

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

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 through a reference sale.

Cisco TAC does not support hardware 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 *Cisco BTS 10200 Softswitch Release Notes*. Cisco TAC supports only BTS 10200 systems running on these Cisco-specified hardware configurations. The software is not supported on any other types or combinations of hardware.

Cables

The procedures for connecting the intershelf cables (those that connect the various host machines and Ethernet Switches within the BTS 10200) are documented in the *Cabling, VLAN, 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 connections to external NEs are not included with the BTS 10200 order and are customer supplied.

Operator Access

System administrators and operators can access the BTS 10200 using a number of interfaces, including SSH session to the EMS over Ethernet, and OSS and NMS connections. Communications can be interactive or in batch mode (batch mode uses SFTP). See the "EMS Functions" section on page 1-14 for additional user interface options.

CHAPTER 2

Supported Signaling Protocols

Revised: July 2010, OL-23035-01

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

- Media Gateway Control Protocol (MGCP) line
- MGCP Channel-Associated Signaling (CAS)
- Integrated Services Digital Network (ISDN) primary rate interface (PRI)
- Signaling Transport (SIGTRAN) for Signaling System 7 (SS7) applications, including ISDN user part (ISUP) support for several national ISUP variants
- H.323
- H.248 (Line-Side Access Support)
- Session Initiation Protocol (SIP) and SIP-T
- PacketCable-based signaling protocols:
  - Network-Based Call Signaling (NCS) protocol
  - Trunking Gateway Control Protocol (TGCP)
  - Dynamic quality of service (DQoS)/Common Open Policy Service (COPS) query and response protocol
  - Remote authentication dial-in user service (RADIUS) authentication protocol (IETF RFC 2865)

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

Caution Some signaling features involve the use of other NEs deployed in the service provider network, for example, gateways, media servers, announcement servers, embedded multimedia terminal adapters (eMTAs), H.323 endpoints, and SIP phones. See the "Component Interoperability" section of the *BTS 10200 Release Notes* for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the BTS 10200 Release 7.0 software. Earlier or later releases of platform software might be interoperable with the BTS 10200 and it might be possible to use other functions on these platforms. The list in the *Cisco BTS 10200 Softswitch Release Notes* certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the BTS 10200.

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

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) set up the connections and calls.

The BTS 10200 connects to a variety of MGWs using MGCP, and provides 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 Media Gateway Profile (mgw-profile) table are used to identify the MGCP version and variant that an MGW supports.

General Functions of the 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 BTS 10200 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 BTS 10200 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 BTS 10200).
  - 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.

  Several codec types are supported, including the following ITU-T standard codecs:
  - 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
  - Additional codecs—See the QoS table in the Cisco BTS 10200 Softswitch CLI Database for a complete list.
- MGCP keepalive signaling—The BTS 10200, if provisioned for keepalive function, determines the connectivity status between itself and each MGW. It executes a keepalive process that includes the transmission of audit-endpoint (AUEP) messages to MGCP, TGCP, and NCS based MGWs. There are several provisionable parameters that you can adjust if there are network bandwidth or reliability issues, or if a MGW is slow in responding to commands from the Call Agent. To provision and use this feature, see the "System Usage of MGW Keepalive Parameters" in the *Cisco BTS 10200 Softswitch Troubleshooting Guide*.
- 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 BTS 10200 specifies the preferred reservation profile to the gateway. Whether or not RSVP is used depends on the configuration of the gateway as well as the preferred reservation profile specified by the BTS 10200. 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 BTS 10200. The announcement server interfaces with the BTS 10200 using MGCP. Every BTS 10200 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-based layer that allows multiple applications to have data converted to and from an ATM cell. It uses a protocol that translates data for higher-layer services into the size and format of an ATM cell.

MGCP CAS Signaling Support

The BTS 10200 supports the following MGCP CAS interfaces:

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

Note CAS is used with the MGCP interworking function.

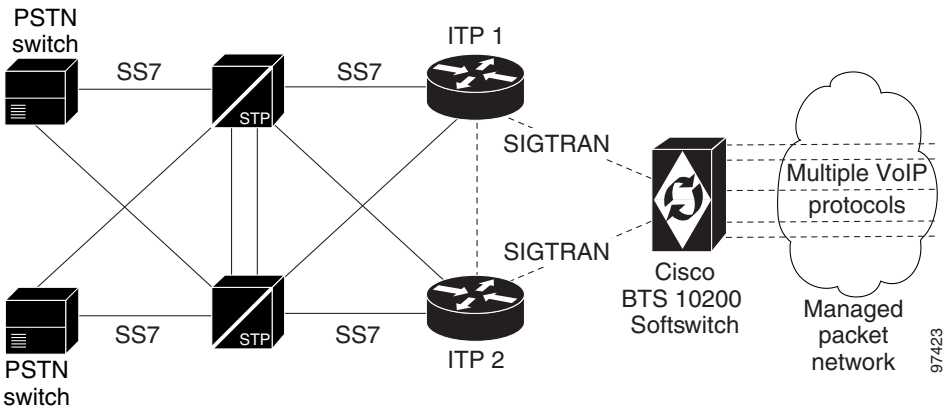
SS7 Signaling Support Through SIGTRAN

The BTS 10200 communicates with 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 BTS 10200 for this purpose.

Interface to the SS7 Network

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

Figure 2-1 BTS 10200 Interface to the 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 BTS 10200 can be configured to have multiple originating point codes (OPCs). For information on OPCs, network configuration options, and subsystems, see the *Cisco BTS 10200 Softswitch SS7 SIGTRAN Guide*.

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)*
- Telcordia standard GR-317-CORE, *Switching System Requirements for Call Control Using the Integrated Services Digital Network User Part*
- Telcordia standard GR-394-CORE, *Switching System Generic Requirements for Interexchange Carrier Interconnection Using the Integrated Services Digital Network User Part*
- Telcordia standard GR-533-CORE, *LSSGR: Database Services Service Switching Points–Toll-Free Service*
- Telcordia standard 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 BTS 10200 supports the following ISUP variants.

Note Q.761 and Q.767 are ITU-T standards.

- ANSI ISUP for North American Numbering Plan (NANP) region, based on Telcordia document GR-317)
- ITU93 White Book ISUP
- European Telecommunications Standards Institute (ETSI) v2 ISUP
- Q.761 Standard
- Q.761 China
- Q.761 Thailand
- Q.761 ETSI v3 Hungary
- Q.761 Standard 97
- Q.761 ETSI v3 France
- Q.761 ETSI v3 Poland
- Q.767 Standard
- Q.767 Mexico
- Q.767 Colombia

- Q.767 Turkish (Release 6.0, Maintenance Release 1 and later)

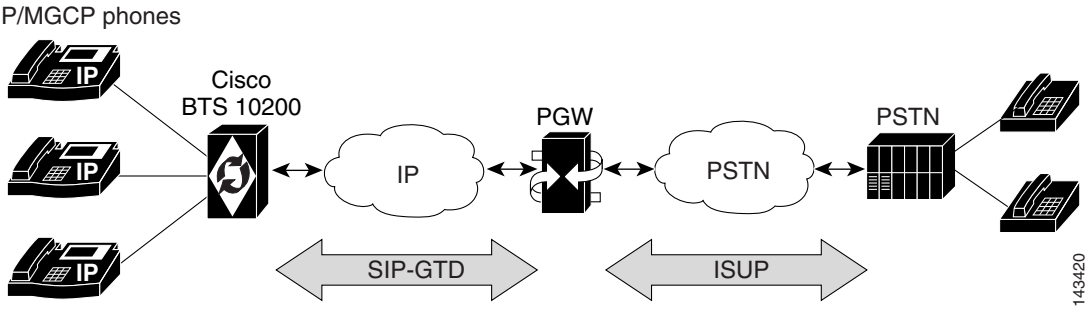
ISUP Transparency with the Cisco PGW 2200

ISUP transparency provides the capability for the BTS 10200 to transfer Generic Transparency Descriptor (GTD) messages and information elements across an IP network to a Cisco PGW 2200. In the Cisco PGW 2200, the GTD messages are mapped to ISUP messages, repackaged, and sent out to the PSTN/SS7 network. ISUP transparency is important because it enables the transport of calls from a SIP network through an IP network and out to a PSTN network without any loss of signaling information. ISUP transparency is achieved with the use of the Cisco GTD mechanism. GTD provides a means to specify messages of various protocols used in the PSTN network in plain text format. In that format, they can be easily understood by the NEs within the IP network or on the boundary between the PSTN and IP networks.

Note This feature is supported in Cisco PGW Software Release 9.6(1) and BTS 10200 Software Release 6.0 and later.

The ISUP transparency function on the BTS-PGW interface, illustrated in Figure 2-2, passes normalized parameters to expedite mapping at the PSTN interconnect side and any feature invocation necessary on either the Cisco PGW 2200 or the BTS 10200. It adds support for GTD attachments to SIP-T trunk messages, allowing the BTS 10200 to interwork with the Cisco PGW 2200 for interconnection to the PSTN.

Figure 2-2 ISUP Transparency on the BTS-PGW Interface



When the BTS 10200 generates SIP messages to be sent out on SIP-T trunks, a GTD attachment is generated based on the GTD parameters defined in the GTD-PARMS token in the Softswitch Trunk Group Profile (softsw-tg-profile) table. The Cisco PGW 2200 decodes GTD attachments of incoming SIP messages, and converts all GTD parameter contents to the equivalent ISUP values in the appropriate information element on the outgoing PSTN side.

When the egress trunk is a SIP-T trunk, the system supports the mapping of Progress Indication messages from the BTS 10200 to SIP INFO messages with GTD attachments containing Call Progress (CPG) messages. This supported feature applies only to SIP subscribers. When a SIP INFO or RE-INVITE message is received over a SIP-T trunk with a GTD attachment containing a CPG message, a Progress Indication message is generated and sent to the system.

In the deployment model, the Cisco PGW 2200 is the PSTN gateway, and the BTS 10200 provides a residential or Centrex application platform.

PSTN Supplementary Services

The following PSTN supplementary services are enabled by the ISUP transparency feature:

- Number ID supplementary services
  - Direct Dial In (DDI)
  - Calling Line Identification Presentation (CLIP)
  - Calling Line Identification Restriction (CLIR)
- Call diversion supplementary services
  - Call Forwarding Busy (CFB)
  - Call Forwarding No Reply (CFNR)
  - Call Forwarding Unconditional (CFU)
  - Call Waiting (CW)
  - Call Hold (HOLD)
- Multiparty supplementary services
  - Three-Party Service (3PTY)
- Transparency requirements
  - Ability to provision which parameters are transported over GTD
  - Call Forwarding No Answer (CFNA)
  - Call Waiting (CW)
  - Call Transfer (SIP Refer is not supported with SIP subscriber Hold signaling)
  - Ability to correlate billing records
- Functionality provided by the Cisco PGW 2200
  - Number Portability (NP)
  - NoA relay
  - Information/Information Request (INF/INR) and Identification Request/Identification Response (IDR/IDS) messaging
  - ITU Method 2 circuit selection
  - NoA modification and routing
  - Calling Party Category (CPC) based routing
  - Ability to modify A-number based on B-number and B-number based on A-number
  - Cause analysis
  - Redirecting A-number screening
  - Virtual VPN behavior
  - Calling Party Number (CGPN) Address Presentation Indicators

Call Progress Signaling for SIP Subscriber on Call Hold

The BTS 10200 can be provisioned to send a call-hold event signal to the other party in the call when a SIP subscriber goes on or off hold. This provisioning is done by means of the SIP-SUB-SEND-CPG-ON-HOLD-SIGNAL token in the Call Agent Configuration (ca-config) table. The default value of this token is N. You must change this value to Y if you want this signal to be sent for all SIP subscribers.

Note The message sent to mute the media path is always sent to the other party, regardless of this flag setting.

Limitations

This feature is subject to the following limitations:

- SIP Refer is not supported with SIP Subscriber Send CPG on Hold Signaling.
- Overdecadic digits are not supported.
- The Cisco PGW 2200 does not send INR messages to the BTS 10200. It responds to INR requests with an INF indication that there is no new information.

GTD Parameters Supported

Table 2-1 shows the GTD parameters supported by this feature and indicates the GTD messages in which each parameter is supported. The values in the GTD Parameter and Name columns of this table are placed in the static Generic Transparency Descriptor Parameter Values (gtd-parm-values) table. You select values from the GTD Parameter column to provision the GTD-PARMS token in the Softswitch Trunk Group Profile (softsw-tg-profile) table.

Enabling a parameter causes it to be encoded in an outgoing GTD attachment of a SIP message on the trunk group if the information is available in the call context.

Only the GTD parameter listed for each GTD message type is decoded when a SIP message with a GTD attachment is received by the system from the network.

For example, the GTD ACL parameter in a GTD REL message will be decoded if it is received, whether it is provisioned or not. However, a GTD UUS parameter received in a GTD REL message is ignored, even if it is provisioned, because it is not in the table.

Table 2-1 GTD Parameters and Supported GTD Messages

GTD Parameter	Name	GTD IAM	GTD ACM	GTD CPG	GTD ANM	GTD CON	GTD REL	GTD SUS	GTD RES
ACL	Automatic Congestion Level	—	—	—	—	—	Yes	—	—
ATP	Access Transport	Yes	Yes	Yes	Yes	Yes	Yes	—	—
BCI	Backward Call Indicators	—	Yes	Yes	Yes	Yes	—	—	—
CAI	Cause Indicators	—	Yes	Yes	—	—	Yes	—	—
CDI	Call Diversion Information	—	Yes	Yes	—	—	—	—	—
CGN	Calling Party Number	Yes	—	—	—	—	—	—	—
CHN	Charge Number	Yes	—	—	—	—	—	—	—
CID	Carrier Identification	Yes	—	—	—	—	—	—	—

Table 2-1 GTD Parameters and Supported GTD Messages (continued)

GTD Parameter	Name	GTD IAM	GTD ACM	GTD CPG	GTD ANM	GTD CON	GTD REL	GTD SUS	GTD RES
CNN	Connected Number		—	—	Yes	Yes	—	—	—
CPC	Calling Party Category	Yes	—	—	—	—	—	—	—
CPN	Called Party Number	Yes	—	—	—	—	—	—	—
CSI	Carrier Selection Information	Yes	—	—	—	—	—	—	—
DIS	Display Information	—	—	—	Yes	Yes	Yes	—	—
EVI	Event Information Indicators	—	Yes	Yes	—	—	Yes	—	—
FCI	Forward Call Indicators	Yes	—	—	—	—	—	—	—
GCI	Global Call Identification	Yes	—	—	—	Yes	—	—	—
GEA	Generic Address	Yes	—	—	—	—	—	—	—
GED	Generic Digits	Yes	—	—	—	—	—	—	—
GEN	Generic Name	Yes	—	—	—	Yes	—	—	—
GNO	Generic Notification	Yes	Yes	Yes	—	—	—	—	—
HOC	Hop Counter	Yes	—	—	—	—	—	—	—
JUR	Jurisdiction	Yes	—	—	—	—	—	—	—
NOC	Nature of Connection Indicators	Yes	—	—	—	—	—	—	—
NSF	Network Specific Facilities	—	Yes	Yes	—	—	—	—	—
OBI	Optional Backward Call Indicators	—	Yes	Yes	Yes	Yes	—	—	—
OCN	Original Called Number	Yes	—	—	—	—	—	—	—
OLI	Originating Line Information	Yes	—	—	—	—	—	—	—
RCT	Redirect Counter	Yes	—	—	—	—	—	—	—
RGN	Redirecting Number	Yes	—	—	—	—	—	—	—
RNI	Redirection Information	Yes	—	—	—	—	—	—	—
RNN	Redirection Number	—	Yes	Yes	Yes	Yes	Yes	—	—
RNR	Redirection Number Restriction	—	Yes	Yes	Yes	Yes	—	—	—
SCI	Service Code Indicator	Yes	—	—	—	—	—	—	—
SRI	Suspend/Resume Indicators	—	—	—	—	—	—	Yes	Yes
TMR	Transmission Medium Required	Yes	—	—	—	Yes	—	—	—
TNS	Transit Network Selection	Yes	—	—	—		—	—	—
UID	UID Indicators	—	Yes	Yes	—	—	—	—	—
UUI	User-To-User Indicators	—	Yes	Yes	Yes	Yes	—	—	—
UUS	User-To-User Information	Yes	Yes	Yes	Yes	Yes	—	—	—

Note Columns in Table 2-1 show the GTD message in which each GTD parameter is supported. This information is for reference only and is not provisionable.

Note UID is only decoded. It is never encoded.

Billing Fields

The BTS 10200 and PGW 2200 produce their own independent billing records. Downstream billing mediation servers use the SIP Call ID to correlate the two records, if required. The SIP Call ID is available in the PGW 2200 call detail record (CDR), tag 4203, and in the BTS 10200 CDR record, fields 116 and 144.

Cause Code Selection Precedence

The system performs cause code selection according to the following order of precedence:

1. SIP header reason code
2. GTD body
3. SIP response code

Troubleshooting

There are no troubleshooting tools created specifically for the transparency feature. Use the existing tools to extract traces from log files on the BTS 10200 and the call trace and siptool capabilities on the PGW 2200. Both tools support ASCII attachments such as the GTD attachment.

Provisioning Procedure

See the "BTS-PGW ISUP Transparency" section in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Additional SIGTRAN and SS7 Information

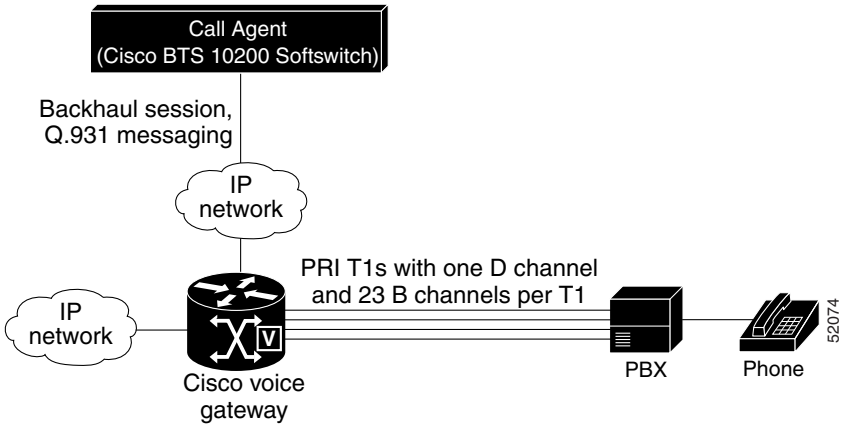
For additional information on provisioning and using SIGTRAN and SS7 protocols on the BTS 10200, see the *Cisco BTS 10200 Softswitch SS7 SIGTRAN Guide*.

ISDN Signaling Support

This section describes the Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) variants and supplementary services supported by the BTS 10200. ISDN PRI allows the BTS 10200 to interconnect to small and medium businesses using legacy PBX PRI interfaces. The basic ISDN NEs and signaling connections are shown in Figure 2-3.

Note Standby elements in the figure are omitted for clarity.

Figure 2-3 Example of ISDN NEs



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 BTS 10200 supports the following capabilities:

- ISDN T1 PRI
- ITU-T standards Q.921 and Q.931 network side
- ISDN backhaul communication of ITU-T standard Q.931 messages from MGWs to the BTS 10200
- Facility Associated Signaling (FAS)
- Non-Facility Associated Signaling (NFAS)
- Backup D channel

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

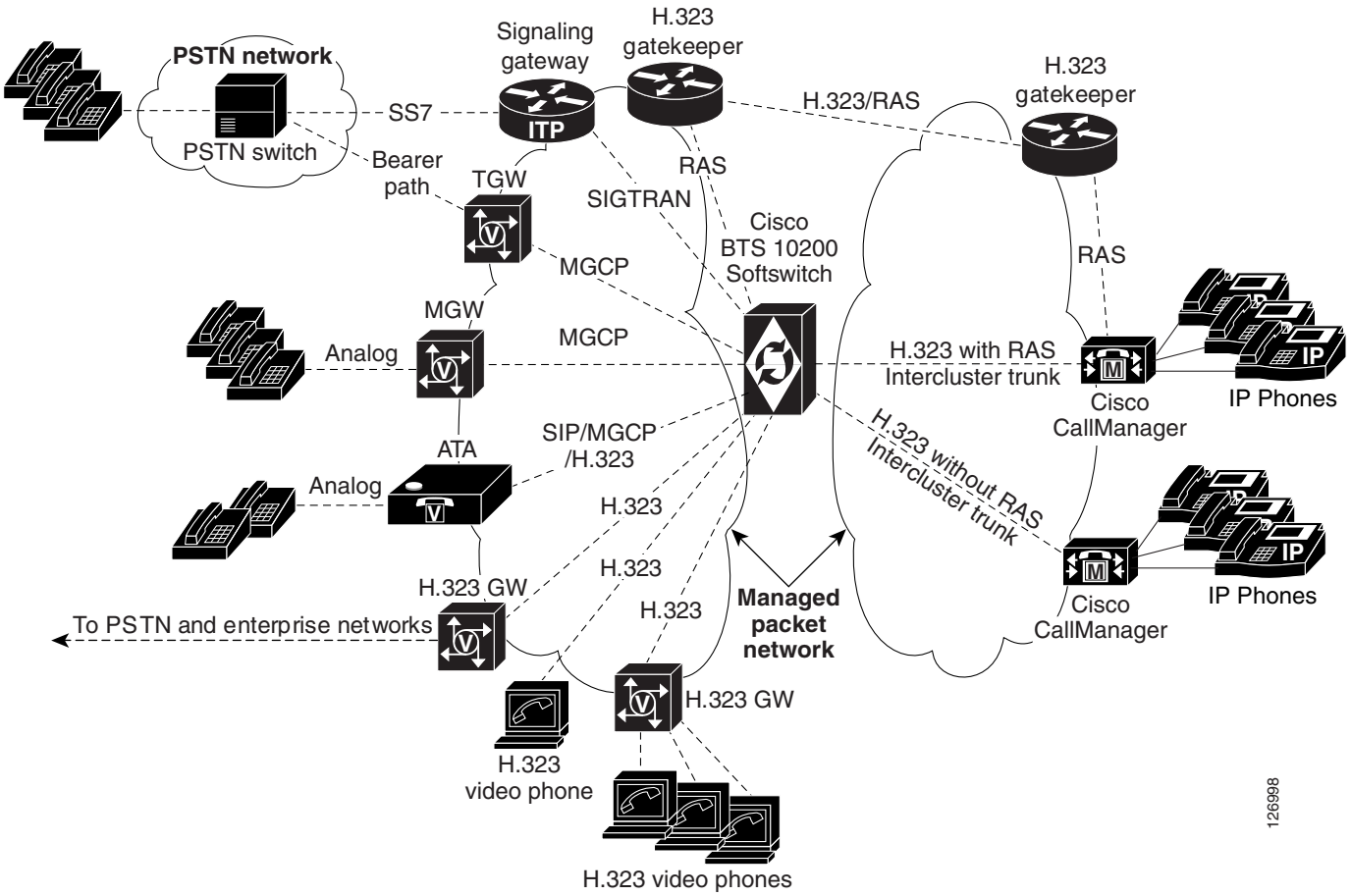
H.323 Signaling Support

The BTS 10200 functions as a logical H.323 gateway to communicate with H.323 gatekeepers (GKs), and with Cisco CallManager and other H.323 gateways. The BTS 10200 also provides signaling for other trunks and lines through MGCP and SIP protocols. In addition, it communicates with 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 2-4.

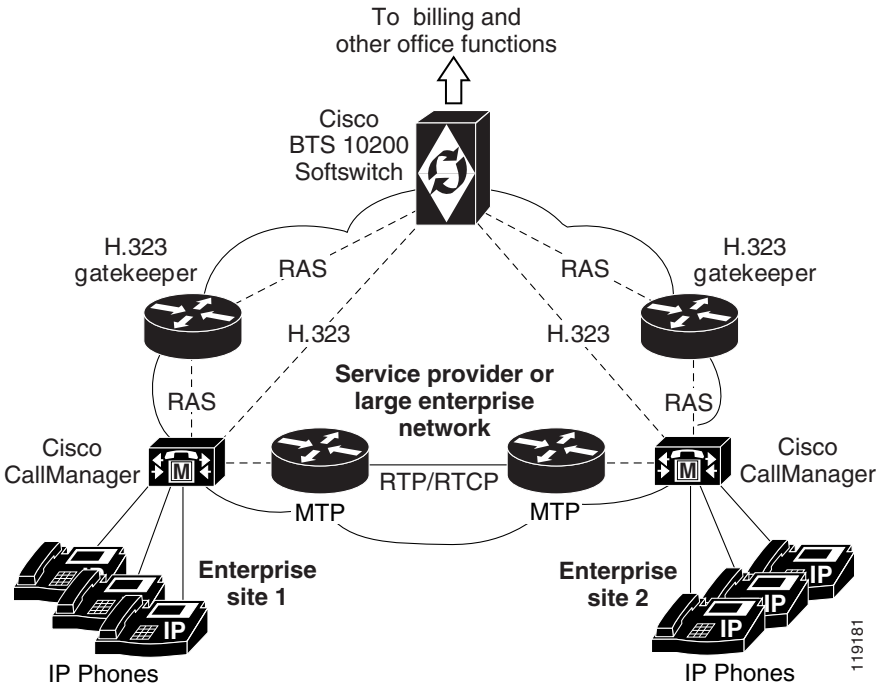
Note You can configure up to four logical H.323 gateways on the BTS 10200.

Figure 2-4 Signaling Links between the BTS 10200, Cisco CallManager, and Other Service Provider NEs



The interoperability between the BTS 10200, 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 BTS 10200 can be used to connect calls between two phones that reside on different Cisco CallManager systems (see Figure 2-5). Signaling of certain information, for example connected name and number information, is transparently passed from the terminating Cisco CallManager to the BTS 10200 and back to the originating Cisco CallManager.

Figure 2-5 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 Guide*.

H.248 Line-Side Signaling Support

The Cisco BTS 10200 Softswitch H.248 Line-Side Access Control feature enables BTS 10200 to use H.248 line-side signaling to communicate with H.248-protocol based network elements. This feature also enables BTS 10200 to provide protocol interworking between H.248 and session initiation protocol (SIP). The support for H.248 Protocol renders necessary protocol interworking to complete voice over packet calls.

The H.248 Line-Side Access Control provides Class-5 features to subscribers behind media gateways (MGWs) interfacing with BTS 10200 using the H.248 protocol. This feature further positions BTS10200 as a switching platform for heterogeneous networks.

Note This feature addresses only the line-side/residential gateway support of H.248 protocol interface, and the features set applicable to line-side.

The Megaco/H.248 protocol is the international standard for media gateway controller (MGC)/MG device control protocol developed jointly by both IETF and ITU-T open standards bodies.

Cisco BTS 10200 Softswitch in H.248 Packet Network

The H.248 line-side access control feature provides a gateway control interface between the Cisco BTS 10200 Softswitch and the H.248 supported Media Gateways. This new interface is based on the ITU-SG16/IETF specification of H.248 which defines a decomposed gateway architecture. This architecture is composed of the following:

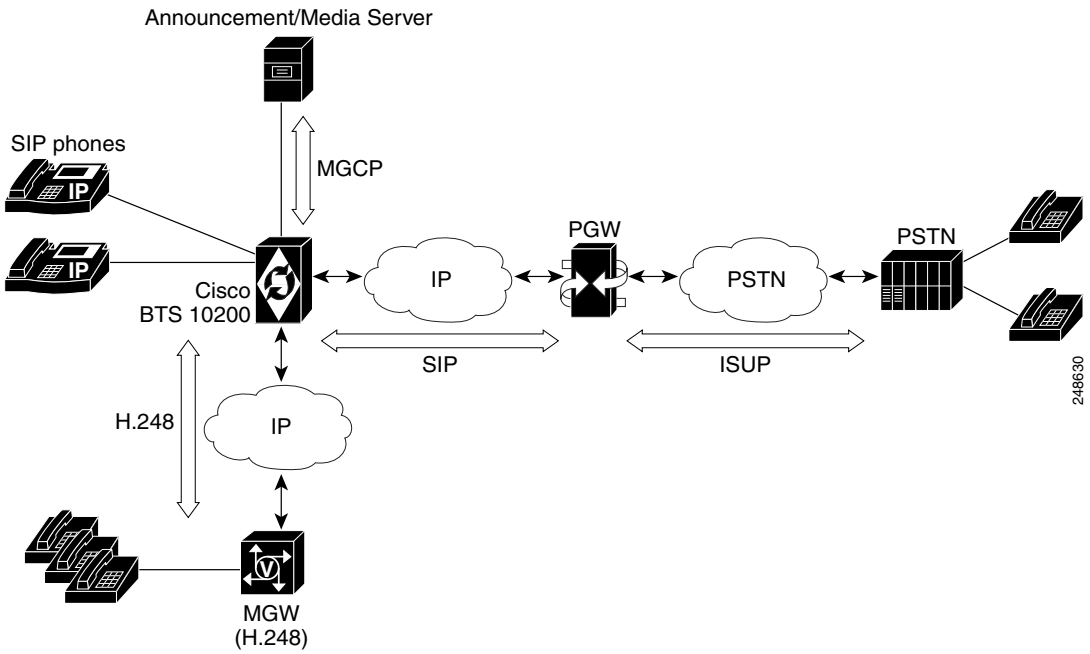
- An MGC, an intelligent entity that manages the establishment and tearing down of calls.
- A MGW, a simple entity that responds to the MGC requests and independently processes media streams.
- A distributed call control functionality between an MGC and an MGW. The MGC sends commands to the MGW using the H.248 protocol.

BTS 10200 supports media gateway control protocol (MGCP) which is based on IETF Informational RFC 2705/3435 as a MGC/MG device control protocol to the media gateways. On the other hand, H.248 is an IETF official standard MGC/MG device call control protocol.

Release 7.0 adds H.248 as another MGC/MG call control protocol in addition to the existing support for MGCP. Independently, both Megaco/H.248 and MGCP can co-exist and run on the same BTS10200 platform at the same time. However, Release 7.0 does not provide call interworking between MGCP and H.248. For H.248 subscriber announcement support, limited interaction with MGCP is provided, because BTS 10200 supports announcements based only on MGCP interface.

Figure 2-6 shows a network architecture example in which BTS 10200 provides native support for H.248 subscribers. As shown in the figure, BTS 10200 can establish calls between networks with various protocols, including calls between H.248 subscribers.

Figure 2-6 Example of a BTS 10200 in the H.248 Network



The Cisco BTS 10200 Softswitch H.248-based functions can be used on managed H.248 networks that contain the Cisco BTS 10200 Softswitch and the following network element types:

- H.248-based IP PBX systems

- Analog phones connected to H.248 Access/Media Gateways

SIP and SIP-T Signaling Support

The BTS 10200 uses SIP) and SIP for telephones (SIP-T) signaling to communicate with other SIP-based NEs. 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 functions on the BTS 10200. For additional details of the BTS 10200 SIP implementation and applicable procedures, see the *Cisco BTS 10200 Softswitch SIP Guide*.

SIP Functions

The BTS 10200 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 BTS 10200 automatically acts as a back-to-back UA when there is a SIP-to-SIP call.

- SS7 bridging between softswitches by means of SIP-T methods
- Native support of SIP endpoints such as SIP phones, including authentication and registration management. (For example, the BTS 10200 maintains the current location of SIP subscribers.)
- Verification of the SIP REGISTER message to ensure that it came from a provisioned endpoint

SIP roles performed by the BTS 10200 include:

- User agent server (UAS)
- User agent client (UAC)
- Registrar
- SIP subscriber authentication

SIP Features

The BTS 10200 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 BTS 10200 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 Telcordia standard 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 functions are described in IETF RFC 3398, *Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping*.

FCP Interface

The BTS 10200 uses Feature Control Protocol (FCP) for internal communications between the CA and 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 BTS 10200 provides call data for billing on SIP calls. Specific fields are supported in the call detail records for calls that originate or terminate on a SIP trunk or subscriber line. For detailed information on billing management and data, see the *Cisco BTS 10200 Softswitch Billing Interface Guide*.

SIP and SIP-T References

The BTS 10200 SIP implementation is based on the evolving standards in the IETF RFC publications, and may not be fully compliant in all cases. The BTS 10200 is largely compliant with RFC 3261. For the level of compliance with other RFC publications and drafts, see the specific feature descriptions in the *Cisco BTS 10200 Softswitch SIP Guide*.

PacketCable-Based Signaling Support

This section summarizes BTS 10200 support for PacketCable-based signaling and includes the following topics:

PacketCable-Based Functions

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

The BTS 10200 provides call control, call routing, and signaling for several types of NEs:

- Multimedia terminal adapters (MTAs) and eMTAs
- Cable modem termination systems (CMTSs)
- TGWs

The BTS 10200 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 functions.

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

- NCS protocol.
- TGCP.

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

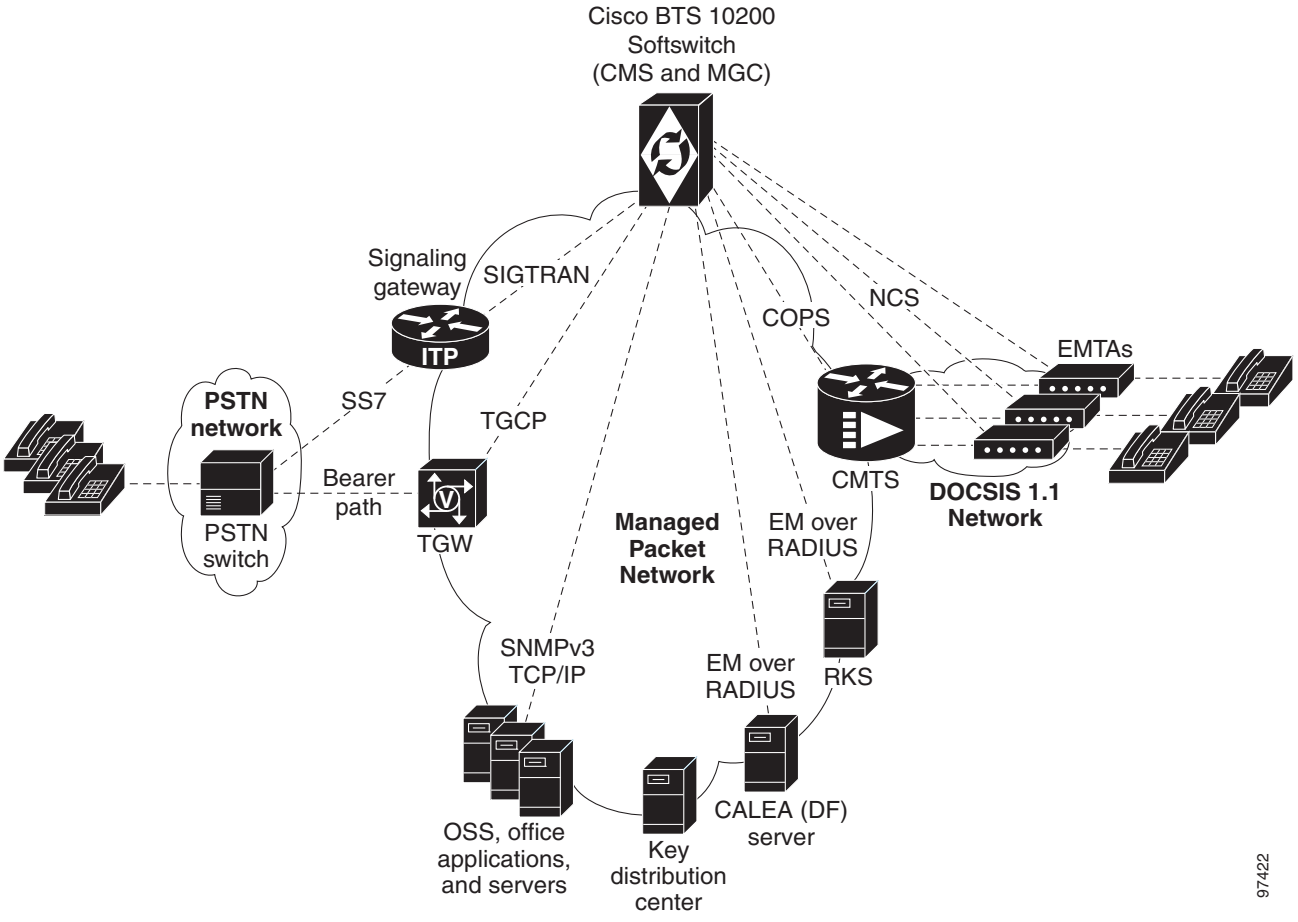
- DQoS/COPS query and response protocol.
- RADIUS authentication protocol (IETF RFC 2865), used for transmission of event messages (EMs) to an external RKS for billing purposes.

- Security features, including implementation of IP security (IPsec) architecture, key management using Internet Key Exchange (IKE) and Kerberos, and encryption of certain IPsec keys.
- Interface for support of lawful intercept and the Communications Assistance for Law Enforcement Act (CALEA). See the "Lawful Intercept Interface" section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions Guide* for a description of this feature.

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

Figure 2-7 shows a typical network with PacketCable-based NEs and the applicable external interfaces of the BTS 10200.

Figure 2-7 Example of PacketCable-Based Network Architecture



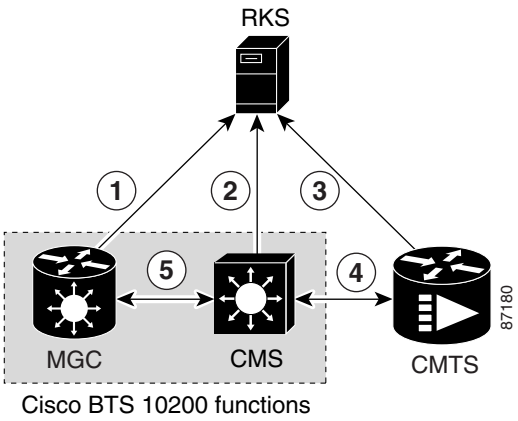
Event Message Implementation

This section describes the implementation of the event message (EM) feature on the BTS 10200. 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 BTS 10200 (which performs the CMS and MGC functions) transfers EMs to an external RKS that assembles call detail records (CDRs) from the EMs.

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

Figure 2-8 illustrates the PacketCable NEs and interfaces involved in the generation and processing of EMs.

Figure 2-8 Event Message Interfaces



Notes for Figure 2-8

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

Note For additional technical discussion, prerequisites, and provisioning steps, see the *Cisco BTS 10200 Softswitch PacketCable 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, described in the following documents, 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 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 BTS 10200 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 by use of CLI commands.

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

GLOSSARY

Revised: July 2010, OL-23035-01

This glossary includes acronyms and terms used in this document, along with a number of terms used in other Cisco BTS 10200 Softswitch documentation and the voice-over-IP industry.

A

AAA	Authorization, Authentication, and Accounting
AC	automatic callback
AC_ACT	automatic callback activation
AC_DEACT	automatic callback deactivation
ACG	automatic call gap
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

AUEP audit-endpoint

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

BIND Berkeley Internet Name Daemon

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
CAD	CORBA adapter interface
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 detail 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; 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
CVR	circuit validation response
CVT	circuit validation test
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 system

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)

DQoS dynamic quality of service

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)

eMTA Embedded multimedia terminal adapter

EPOM Extensible Provisioning and Operation Manager

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, and 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 (IP) 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

KDC key distribution center

L

LAF log archive file

LAN local area network

LATA local access and transport area

LCD limited call duration

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

MGA media gateway adapter

MGC media gateway controller

MGCP Media Gateway Control Protocol

MGW 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 Multimedia terminal adapter

MTP Message transport part

MTU maximum transmission unit

MWI message waiting indicator

N

NANP North American Numbering Plan

NANPA North American Numbering Plan Administration

NAS network access server

NCS Network-Based Call Signaling protocol

NE network element

NEBS Network Equipment Building Standards

NFAS Non-Facility Associated Signaling

NIS network information service

NMS network management system

NO network operator

NOA nature of address

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
QVT	query verification tool

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

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)
SG	signaling gateway
SGCP	Simple Gateway Control Protocol
SIA	SIP adapter
SID	system identification number
SIGTRAN	Signaling Transport
SII	Cisco Service Independent Intercept architecture
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
SPA	Self-Service Phone Administration
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

TGCP Trunking Gateway Control Protocol

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

TVT translation verification tool

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

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

X