CHAPTER 1

Cisco BTS 10200 Softswitch Technical Overview

Revised: February 7, 2008, OL-11755-03

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

Tip The companion to this document is the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document. That document contains descriptions of network features, subscriber features, class of service (CoS) functions, outgoing call barring (OCB), feature interactions, and interactive voice response (IVR) features.

In previous releases, the *System Description* contained information on site preparation and network communications requirements. That preinstallation information has been moved to a new document, *Cisco BTS 10200 Softswitch Site Preparation and Network Communications Requirements*.

Introduction

The Cisco BTS 10200 Softswitch is a software-based, class-independent network switch. It provides call-control intelligence for establishing, maintaining, routing, and terminating voice calls 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 Cisco BTS 10200 Softswitch provides the major signaling functions performed by traditional Class 4 and Class 5 switching systems in the PSTN. It also provides more than 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 Cisco BTS 10200 Softswitch application software is installed on Cisco specified host machines, it creates a set of logical components. Together these logical components provide all of the features and functions of the Cisco BTS 10200 Softswitch. The disk drives in the host machines store the provisioned database and system-generated data. These logical components and the Cisco specified hardware are described later in this chapter.

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

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

When you order the Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch software is installed on your system. Details of the software installation are provided in the *Cisco BTS 10200 Softswitch Application Installation Procedure*.

Cisco BTS 10200 Softswitch in the TMN Model

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

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

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

Overview of Features and Functions

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

- Network Features and Functions, page 1-5
- 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 MGCP, SIGTRAN (for SS7), H.323, PacketCable, Session Initiation Protocol (SIP), ISDN, and Channel-Associated Signaling (CAS).
- PSTN-parity routing mechanisms for voice calls, including local, national, international, operator services, and emergency services routing. (In North America, this includes local access and transport area (LATA) calls and interLATA calls.)
- Support for the following types of calls:
  - PSTN-to-packet network calls—Calls that originate on a PSTN network and terminate on a packet network (off-net calls)
  - Packet-to-PSTN network calls—Calls that originate on a packet network and terminate on a PSTN network (off-net calls)
  - Packet-to-packet calls—Calls that originate and terminate on a packet network (packet on-net calls)
  - PSTN-to-packet-to-PSTN calls—Calls that originate on an ingress PSTN circuit and travel over a packet network to terminate on an egress PSTN port
- Support for the following types of routing, configurable 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 Cisco BTS 10200 Softswitch 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 five times. (Any TG in the list that is administratively out of service is not counted as an attempt.) If all five attempts fail, the call is released, and the system provides a release announcement.
- Digit manipulation function, which enables the Cisco BTS 10200 Softswitch to modify the calling party dial number, called party number, and nature of address (NOA) for both incoming and outgoing calls. This feature supports the use of:
  - North American Numbering Plan (NANP)

  - ITU-T E.164 numbering plan
  - ANI- or DNIS-based routing

Note The calling party number is 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 (Cisco BTS 10200 Softswitch) and the remote switch (the switch at the far end of the applicable trunk group).
  - Supports sending and receiving CLLI code in circuit validation response (CVR) messages. CVR messages are generated in response to a circuit validation test (CVT) message.
- Control of announcement servers.
- Communications with interactive voice response (IVR) servers.
- SIGTRAN-based communications with signaling gateways (SGs) that provide SS7 signaling and interoperability with legacy PSTN equipment.
- Support for several national ISUP versions.
- Support for ISUP transparency with the Cisco PGW 2200.
- Interoperability with PBX equipment through the ISDN-PRI and Channel-Associated Signaling (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), Network-Based Call Signaling (NCS) protocol, and Trunking Gateway Control Protocol (TGCP) signaling, as well as IPsec and dynamic quality of service (DQoS) features.
- T.38 fax relay.
- Public safety answering point (PSAP) support for enhanced 911 emergency services.

- Interfaces for support of the Communications Assistance for Law Enforcement Act (CALEA), in both PacketCable and Cisco Service Independent Intercept (SII) architectures.
- Support for the automatic call gap (ACG) function with service control point (SCP) query.
- Provisionable option to suppress sending of Internet Control Message Protocol (ICMP) ping. The service provider can enable or disable the sending of ICMP pings to MGWs. The Cisco BTS 10200 Softswitch sends an ICMP ping only when an audit-endpoint (AUEP) attempt fails.
- 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 Cisco BTS 10200 Softswitch.
- 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.
- (Release 5.0) SIP triggers (provided for MGCP and NCS subscribers only)—The SIP Triggers feature uses the SIP protocol, with some extensions, to enable the Cisco BTS 10200 Softswitch 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.
- (Release 5.0) Call Agent controlled mode for RFC 2833 DTMF Relay—During call setup, the CA (the Cisco BTS 10200 Softswitch) can authorize an embedded multimedia terminal adapter (eMTA) or media gateway (MGW) to invoke RFC 2833 DTMF relay procedures.
- (Release 5.0) Support for PacketCable Multimedia (PCMM)-based quality of service (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.)
- (Release 5.0) 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.
- (Release 5.0) Emergency 911 trunk connection loss alarm—The Cisco BTS 10200 Softswitch is capable of generating a critical alarm of when an emergency trunk resource becomes remotely or locally blocked.

Note See the Chapter 1, "Network Features," in the *Network and Subscriber Feature Descriptions* document 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 Chapter 2, "Subscriber Features", in the *Network and Subscriber Feature Descriptions* document for complete coverage.

- Class of service (CoS) screening and outgoing call barring (OCB). See the Chapter 3, "Class of Service and Outgoing Call Barring Features", in the *Network and Subscriber Feature Descriptions* document 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

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
- (Release 5.0) Metered billing with collection of metered "pulses" from operators signaled to UPC through SPIROU (French ISUP) ITX messages

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

Operations, Maintenance, and Troubleshooting Features and Functions

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

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

Note Data should be backed up on a daily basis and saved to a remote server. Data backup files are needed in the unlikely event that data in both the primary and secondary sides of any platform 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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch. 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 there are any new log files in these trace log directories, LAF transfers them by sftp to an external archive server specified by the service provider.
- (Release 5.0) Automatic shared memory backup (ASMB)—Provides the ability to create a backup copy of the 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.
- (Release 5.0) 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.
- (Release 5.0) Internal Secondary Authoritative DNS Server (ISADS)—A local DNS database that runs on Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch applications.
- (Release 5.0) Maintenance Release 1) 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.
- (Release 5.0) BTSSTAT software utility—Displays the operational status of all components of the Cisco BTS 10200 Softswitch system.
- (Release 5.0) 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.

Note See the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide* or the *Cisco BTS 10200 Softswitch Troubleshooting Guide* for specific operating, maintenance, and troubleshooting 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—See the preface of the *Cisco BTS 10200 Softswitch Command Line Reference Guide* for a description of this functionality.
- 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 Cisco BTS 10200 Softswitch in a consistent, object-oriented model. The CAD interface supports a means of provisioning the Cisco BTS 10200 Softswitch that parallels the CLI adapter capabilities. The system provides a secure socket layer (SSL) transport for the CORBA adapter. For CORBA details, see the *Cisco BTS 10200 Softswitch CORBA Adapter Interface Specification Programmer's Guide*.
- Extensible Provisioning and Operations Manager (EPOM)—EPOM is a web-based application for real-time provisioning of the Cisco BTS 10200 Softswitch that allows authorized users to show, add, modify, and delete system components, and to query the status of the components. Provisioning tasks in Cisco EPOM generally match tasks done using CLI commands, but they are accomplished through a web browser interface. For EPOM details, see the *Cisco Extensible Provisioning and Operations Manager* document.
- (Release 5.0) Support for CMS subscriber provisioning through a 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 Cisco BTS 10200 Softswitch XML requests.

System Administration Features and Functions

The system supports the following system administration features and functions:

- Secure communications using SSH, SFTP, Secure XML, and HTTPS interfaces.
- Hardened Solaris OS—The Cisco BTS 10200 Softswitch runs on Sun Solaris. Processes and utilities in the UNIX system that are unsuitable for use in a softswitch environment have been disabled.
- Login authentication—The Cisco BTS 10200 Softswitch supports administrative login authentication using Lightweight Directory Access Protocol (LDAP) and RADIUS authentication clients. This functionality is applicable to the Cisco Extensible Provisioning and Operations Manager (EPOM) and Cisco Self-Service Phone Administration (SPA). The system can determine if the account is local or off-board, and transfer login responsibility for off-board accounts to the end-user Authorization, Authentication, and Accounting (AAA) servers. This capability is provisionable through command-line interface (CLI) commands.

- 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 Cisco BTS 10200 Softswitch and describes the functions of each component. The information is organized as follows:

List of Logical Components

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

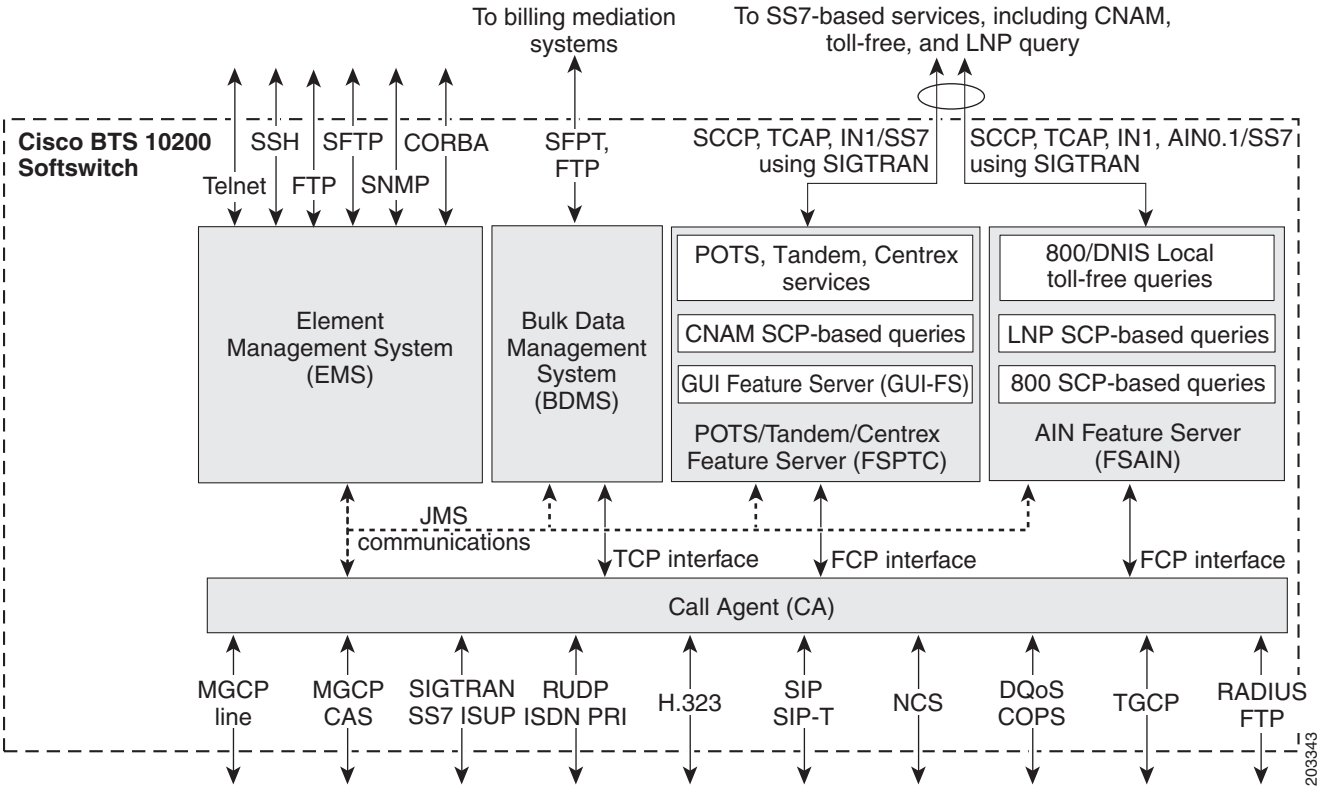
- Call Agent (CA)—Serves as a call management system and media gateway controller. It handles the establishment, processing, and teardown of telephony calls.
- Feature Servers (FSs)—Provide POTS, Tandem, Centrex, and Advanced Intelligent Network (AIN) services to the calls controlled by the CAs. The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

  There are two types of FSs in the Cisco BTS 10200 Softswitch:

  - FSPTC—FS for POTS, Tandem, and Centrex features
  - FSAIN—FS for AIN services
- Element Management System (EMS)—Controls the entire Cisco BTS 10200 Softswitch and acts as a mediation device between an NMS and one or more CAs. It is also the interface for the provisioning, administration, and reporting features of the Cisco BTS 10200 Softswitch.
- Bulk Data Management System (BDMS)—Coordinates the collection of billing data from the CA, and the forwarding of billing records to the service provider billing mediation device.
- Internal Secondary Authoritative DNS Server (ISADS)—The ISADS provides the Cisco BTS 10200 Softswitch with 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 Cisco BTS 10200 Softswitch 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

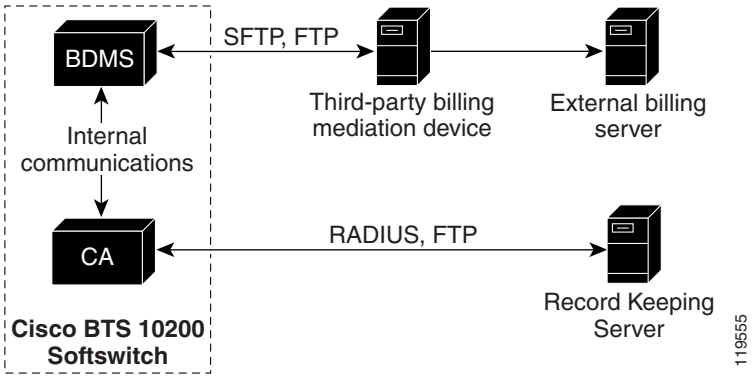
- Provide maintenance primitives for signaling link hardware maintenance and signaling protocol stack provisioning

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 by 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 1-17.
- 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 Cisco BTS 10200 Softswitch.

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 and Event Message Provisioning and Operations Guide.*

FS Functions

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

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

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

The FSs provide access to features through a well defined interface. The Cisco BTS 10200 Softswitch architecture logically separates the FSs (which provide feature control) from the CA (which provides call control). 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 Cisco BTS 10200 Softswitch 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 Specifications* document.

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

EMS Functions

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

- Access the system 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.

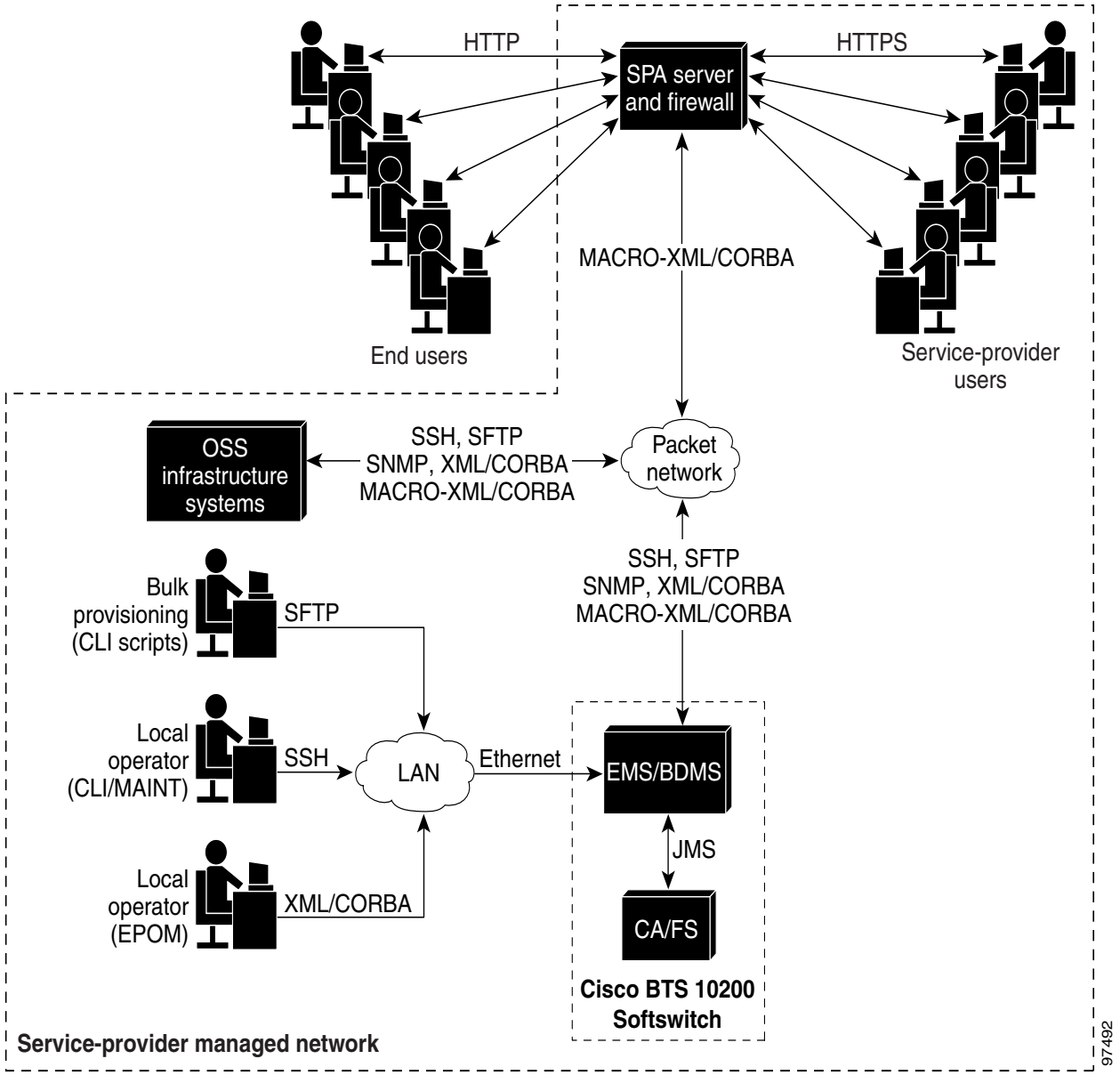
Note For additional information on using these functions, see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*, the *Cisco BTS 10200 Softswitch Provisioning Guide*, and the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide.*

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 Cisco BTS 10200 Softswitch. The core system does not need to interpret the specific data formats used by the other carrier network elements.

EMS Communications

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

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



The user interfaces include the following:

- Secure shell (SSH)—For provisioning 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 Cisco BTS 10200 Softswitch, 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
  - Provisioning through the Cisco Extensible Provisioning and Operations Manager (EPOM) and the Cisco Self-Service Phone Administration (SPA)

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

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

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

Note The functions of the BDMS component, including billing-related communications links, are described in the "BDMS Functions" section on page 1-17.

SNMP Agent

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

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

The SNMP agent supports SNMPv2c operations defined by the opticall.mib Management Information Base (MIB). The MIB is located in the directory /opt/BTSsnmp/etc on the EMS. The NMS needs to load the main MIB (opticall.mib), that 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 Bulk Data Management System (BDMS) stores billing data in the form of call detail blocks (CDBs). CDBs are assembled from billing messages generated in the CA when billing-related call events occur during call processing. The BDMS formats the CDBs into a flat ASCII-file format and transmits them to an external billing collection and mediation device that is part of the service provider billing system (see Figure 1-5). Finally, the BDMS forwards this data to an external billing mediation system or billing server, where it is assembled into CDRs.

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

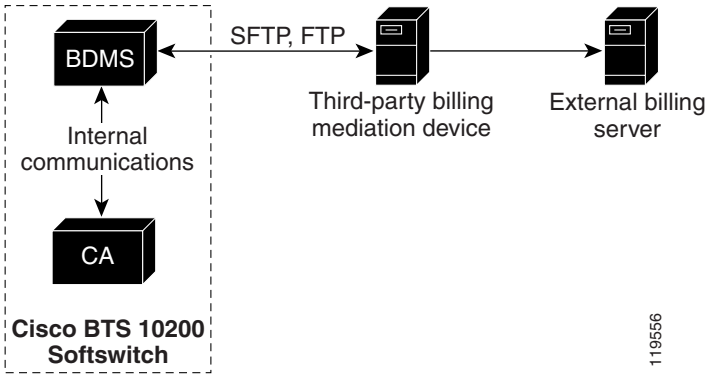
The BDMS provides the following billing functions:

- Supports batch record transmission 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 Cisco BTS 10200 Softswitch.

Figure 1-5 Billing Interface to the BDMS



Internal Secondary Authoritative DNS Server (ISADS)

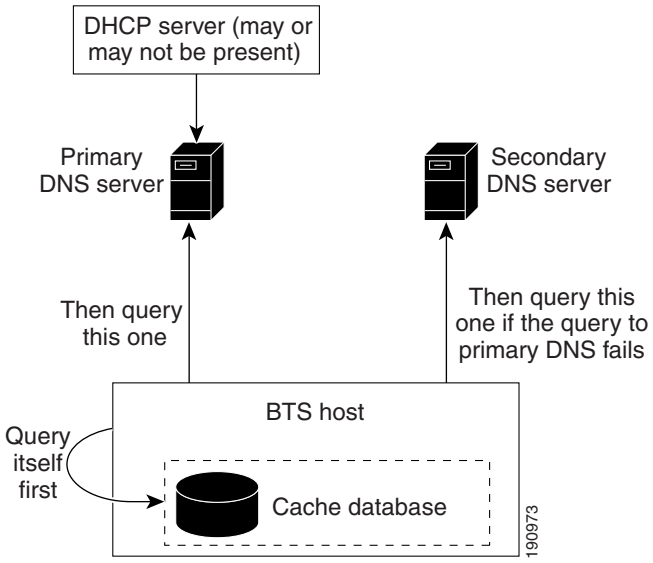
Overview

The internal secondary authoritative DNS server (ISADS) provides the Cisco BTS 10200 Softswitch with an internal DNS database identical to the DNS database in the network. All the domain name queries from the Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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. Cisco BTS 10200 Softswitch 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.

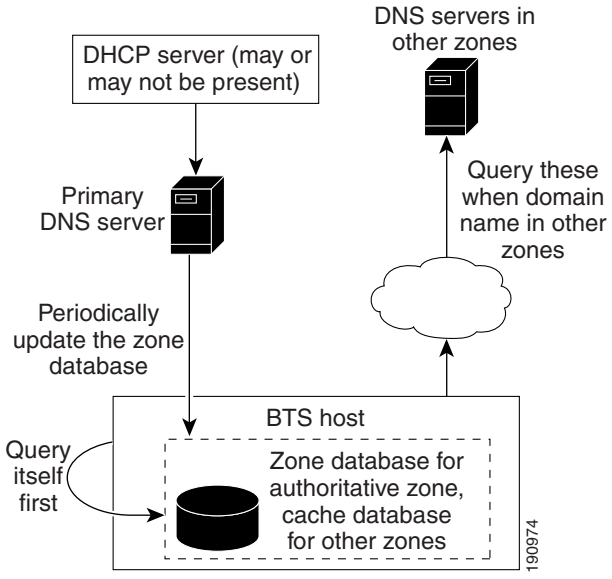
Figure 1-6 Design with Internal Secondary Cache-Only DNS Server



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

When a Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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 New 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 Cisco BTS 10200 Softswitch 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 of the *Application Installation Procedure (Release 5.0)*. For information on how to configure existing systems, refer to Appendix H of the *Application Installation Procedure (Release 5.0)*.

The installation will have a new parameter for the Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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

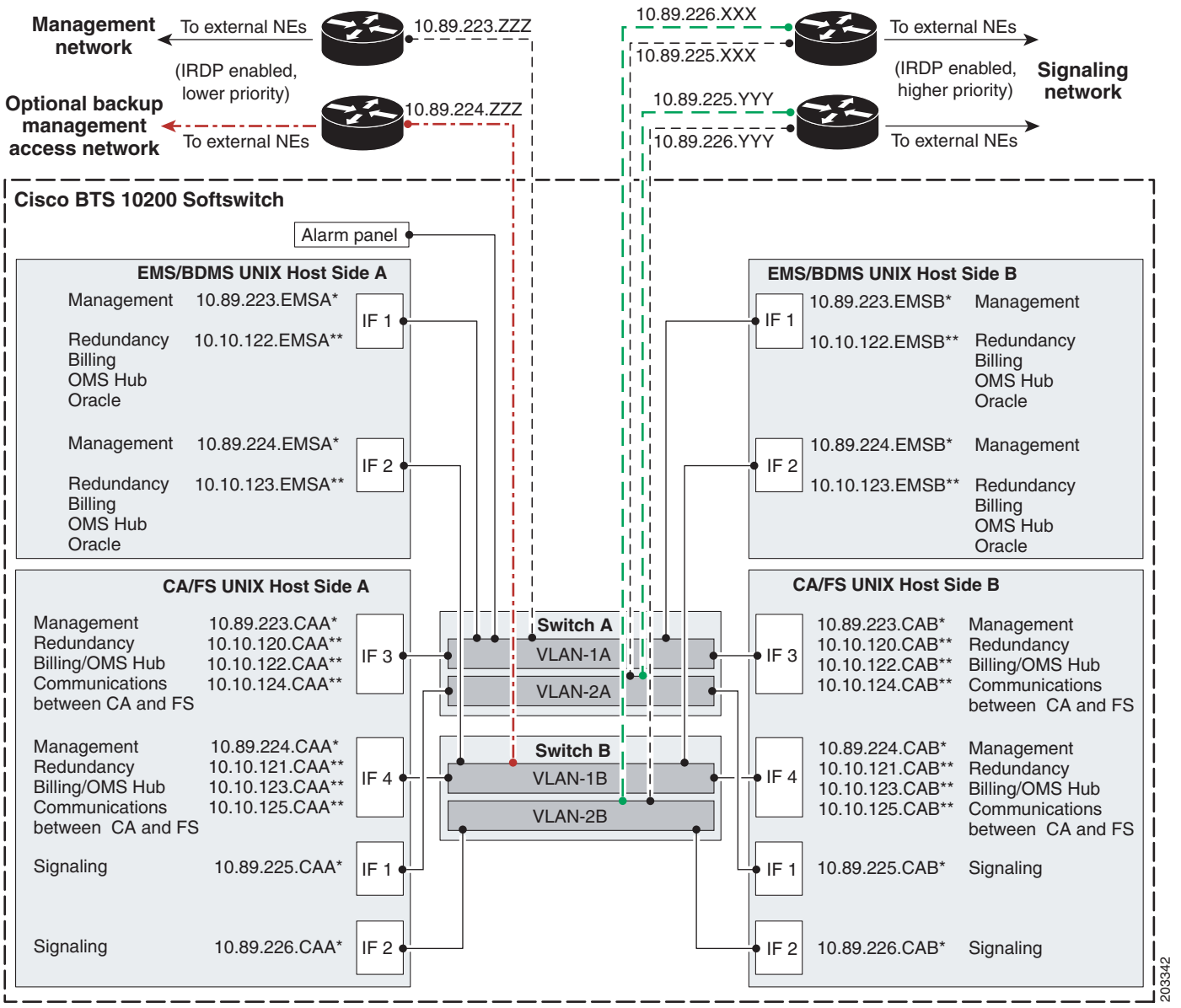
To configure the primary DNS server, refer to Appendix G of the *Application Installation Procedure (Release 5.0)*.

To configure the internal secondary DNS server, refer to Appendix H of the *Application Installation Procedure (Release 5.0)*.

Reliability and Availability of Components

The Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch Network Configuration



Notes for Figure 1-8

1. The following labels represent specific components and functions:

- IF = Interface. The numbers in 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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch.

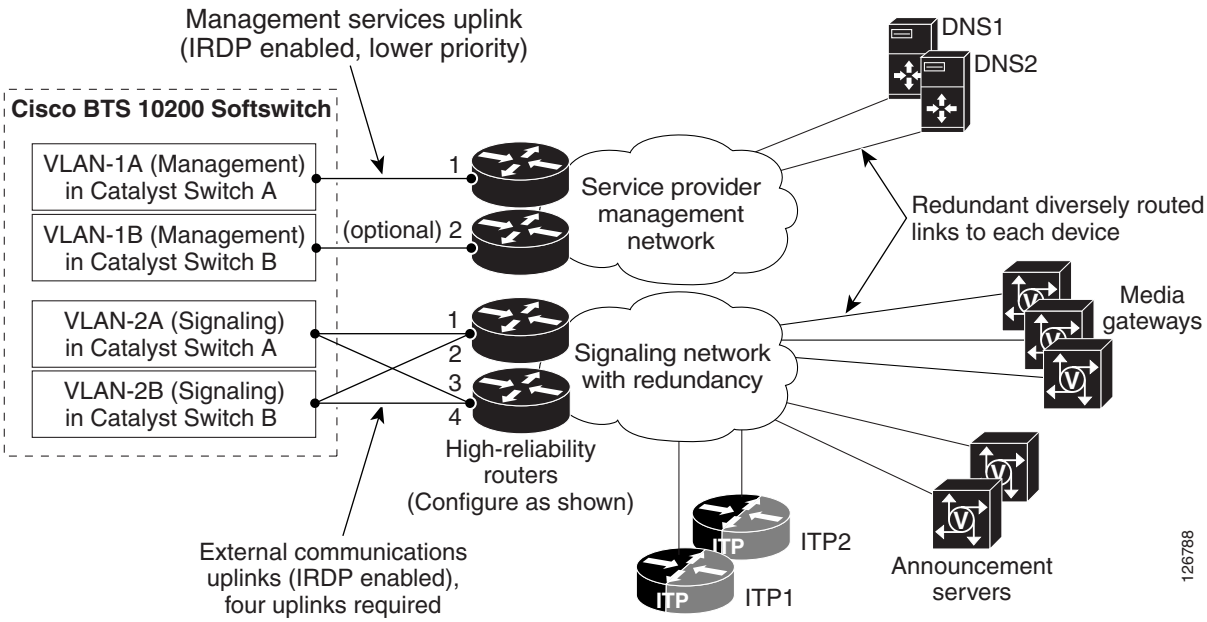
Note The system provides additional support for DNS availability through the internal DNS functionality. See the "Internal Secondary Authoritative DNS Server (ISADS)" section on page 1-18.

8. The alarm panel refers to a terminal server (which could be a terminal server built into an alarm panel). It could be customer supplied or Cisco supplied, depending on the hardware options selected. The alarm panel supplied with some Cisco BTS 10200 Softswitch systems is not used for alarms or for aggregation or reporting of machine alarms; it is used as a form of terminal concentrator. The Cisco BTS 10200 Softswitch software does not transmit machine alarms through this port. Instead, machine alarms are sent 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 Cisco BTS 10200 Softswitch and NEs in the managed network. The initial software configuration of the Cisco BTS 10200 Softswitch enables it to communicate with external NEs.

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

Figure 1-9 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 Cisco BTS 10200 Softswitch, 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 Cisco BTS 10200 Softswitch 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 *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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch 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 Cisco BTS 10200 Softswitch systems running on these Cisco specified hardware configurations. The software is not supported on any other types or combinations of hardware.

Cables

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

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

Operator Access

System administrators and operators can access the Cisco BTS 10200 Softswitch using a number of interfaces, including secure shell (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.