CHAPTER 2

Supported Signaling Protocols

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

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

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

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

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

MGCP Line Signaling Support

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

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

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

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

General Functions of MGCP Interface

The MGCP interface performs the following functions:

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

Special Functions of MGCP Interface

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

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

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

  - G.711 A-law (PCMA)
  - G.723.1 High rate
  - G.723.1 Annex A High rate
  - G.723.1 Low rate
  - G.723.1 Annex A Low rate
  - G.729
  - G.729 Annex B
  - G.726 32K rate
  - G.726 24K rate
  - G.726 16K rate
  - G.728
- Resource Reservation Protocol (RSVP)—An Internet Engineering Task Force (IETF) protocol for providing integrated services and reserving resources on the IP network. The service provider provisions the preferred reservation profile (guaranteed, controlled load, or best effort) in the QoS table. When a reservation is needed on a connection, the Cisco BTS 10200 Softswitch specifies the preferred reservation profile to the gateway. Whether or not RSVP will be done depends on the configuration of the gateway as well as the preferred reservation profile specified by the Cisco BTS 10200 Softswitch. If the best effort RSVP profile is specified, RSVP is not performed.
- Announcement server—A media server that stores network-based announcements and plays them to a caller upon request from the Cisco BTS 10200 Softswitch. The announcement server interfaces with the Cisco BTS 10200 Softswitch using MGCP. Every Cisco BTS 10200 Softswitch in the network requires its own announcement server.
- Dual tone multifrequency (DTMF) signaling—Signaling that is transported across the IP network under MGCP control.
- Channel-associated signaling (CAS)—Signaling that is used with the MGCP interworking function.
- Voice over ATM (VoATM) support—Configurable parameters that support ATM extensions (AAL1, AAL2, and AAL5) on MGCP.

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

MGCP CAS Signaling Support

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

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

Note CAS is used with the MGCP interworking function.

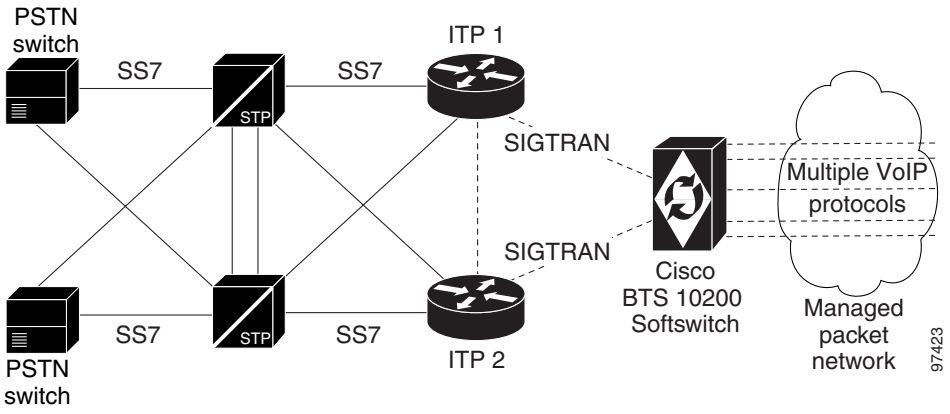
SS7 Signaling Support via SIGTRAN

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

Interface to the SS7 Network

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

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



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

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

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

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

Support for ISUP Variants

The Cisco BTS 10200 Softswitch supports the following ISUP variants:

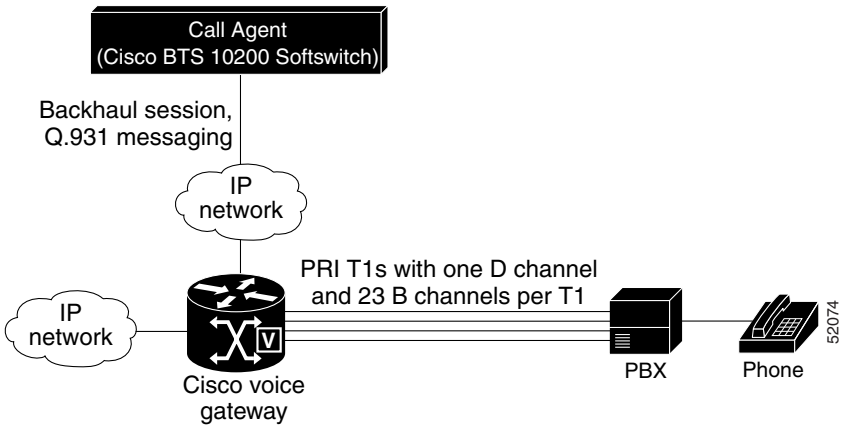
- ITU93 White Book ISUP—Release 4.1 and later
- European Telecommunications Standards Institute (ETSI) v2 ISUP—Release 4.4.1 and later
- ANSI ISUP (for NANP region)—Release 3.5 and later
- China—Release 4.1 and later
- Mexico—Release 4.1 and later

ISDN Signaling Support

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

Note Standby elements in the figure are omitted for clarity.

Figure 2-2 Example of ISDN Network Elements



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

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

The Cisco BTS 10200 Softswitch supports the following capabilities:

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

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

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

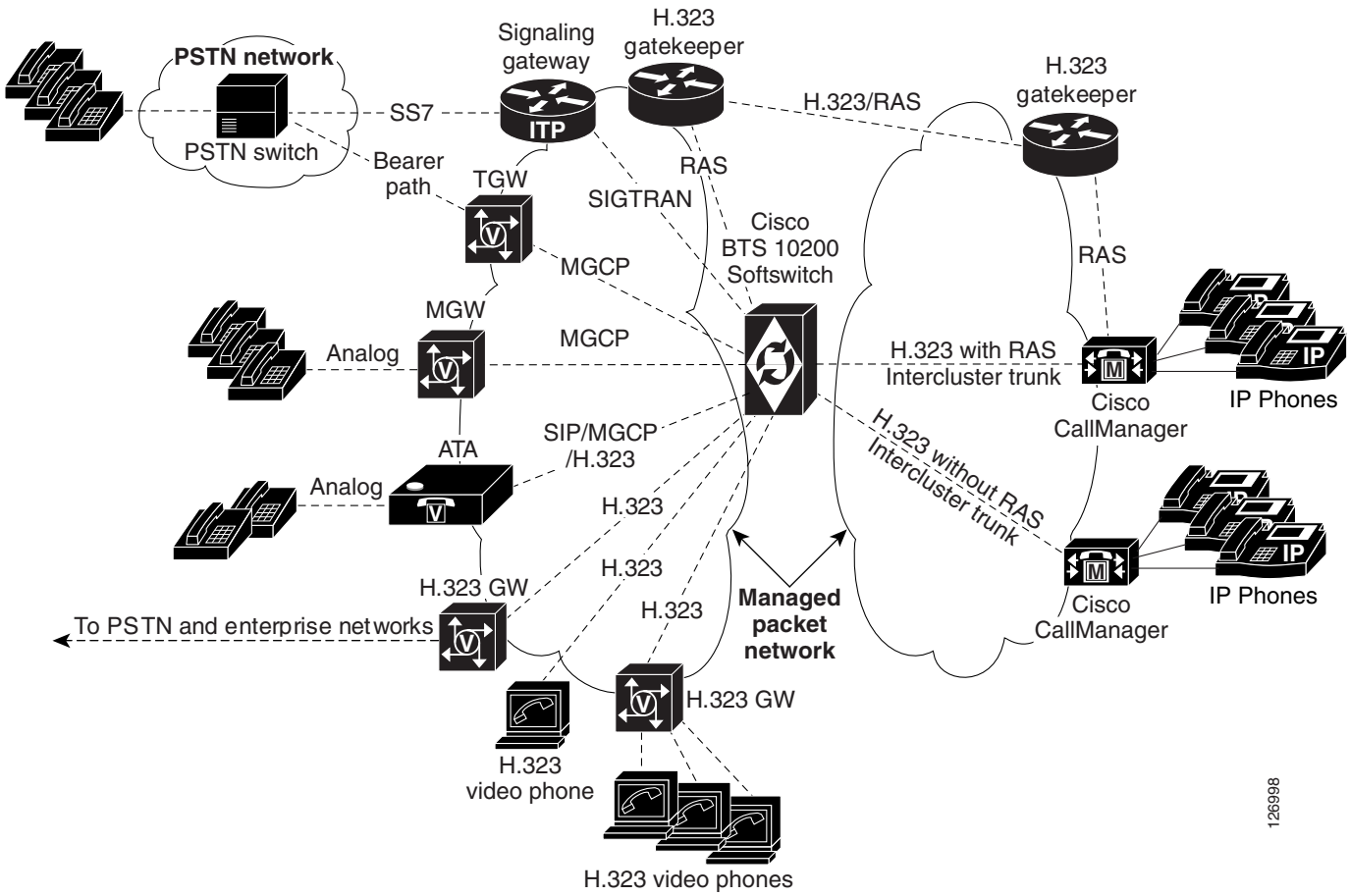
H.323 Signaling Support

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

These signaling links are shown in Figure 2-3.

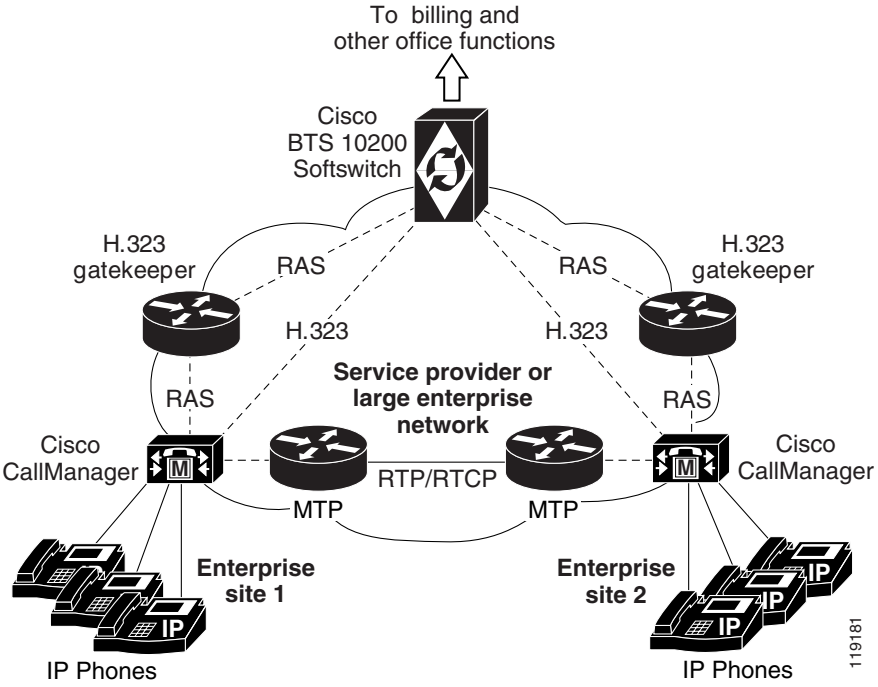
Note The Cisco BTS 10200 Softswitch can be configured as up to four logical H.323 gateways.

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



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

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



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

SIP and SIP-T Signaling Support

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

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

SIP Functions

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

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

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

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

SIP roles performed by the Cisco BTS 10200 Softswitch include:

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

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

SIP Features

The Cisco BTS 10200 Softswitch supports the following SIP features:

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

SIP-T Support

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

FCP Interface

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

SIP Billing Support

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

SIP and SIP-T References

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

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

PacketCable-Based Signaling Support

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

PacketCable-Based Functions

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

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

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

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

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

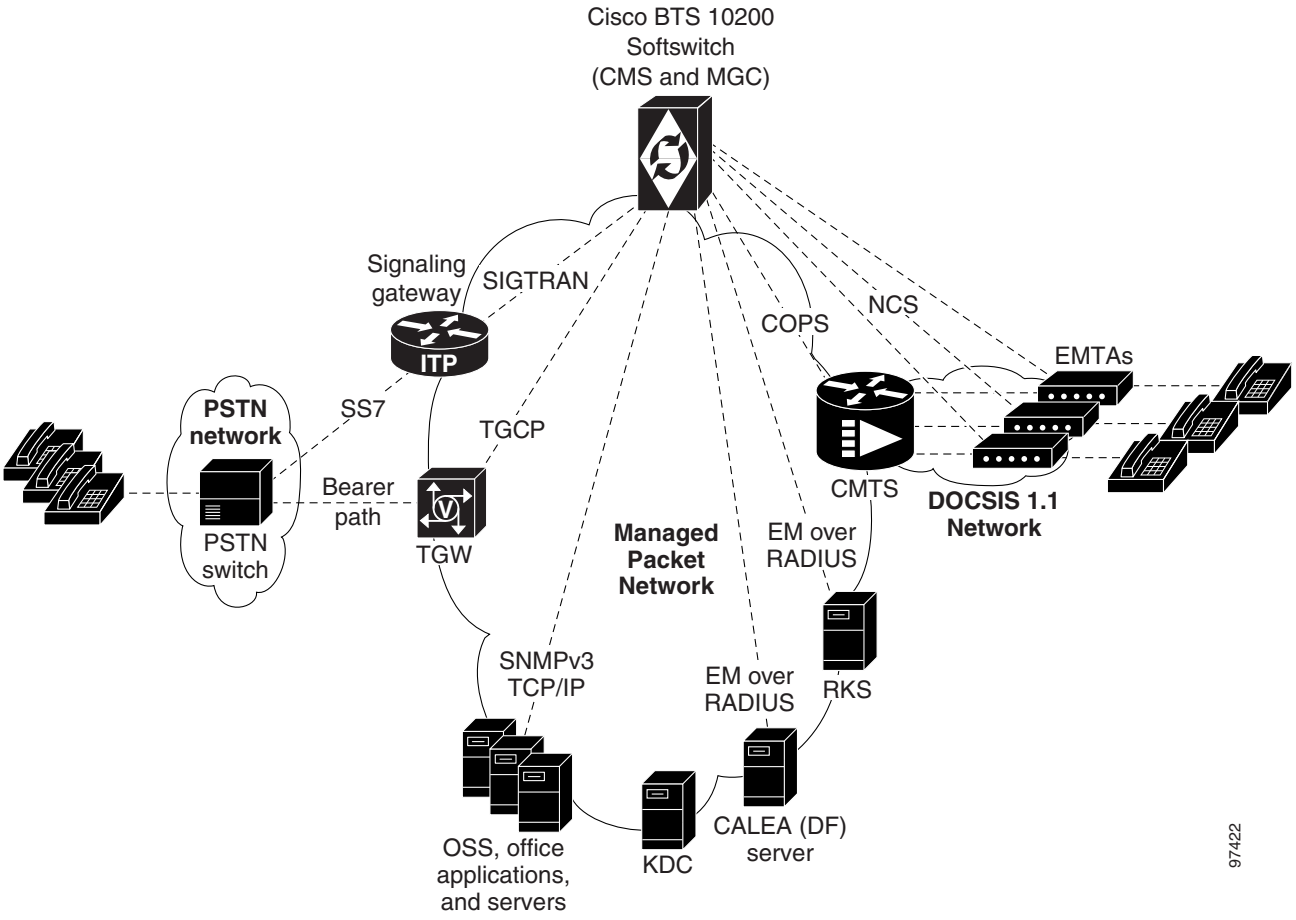
Note NCS protocol and TGCP are based on MGCP; they are referred to as profiles of MGCP.

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

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

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

Figure 2-5 Example of PacketCable-Based Network Architecture



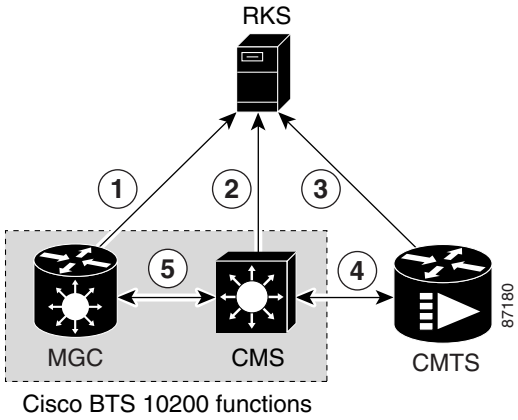
Event Message Implementation

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

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

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

Figure 2-6 Event Message Interfaces



Notes for Figure 2-6:

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

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

Security Implementation

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

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

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

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

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

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