PacketCable and Event Message Provisioning and Operations Guide: Cisco BTS 10200 Softswitch, Release 4.5.x

Revised: March 29, 2007, OL-7313-05

This document describes how the Cisco BTS 10200 Softswitch implements PacketCable-based interfaces and functions. It also provides provisioning and operating information for PacketCable features and event messages (EMs). It is intended for use by service provider management, system administration, and engineering personnel who are responsible for designing, installing, provisioning, and maintaining networks that use the Cisco BTS 10200 Softswitch system in a PacketCable-based network.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Feature History

Release	Modification
Release 4.5.x	Version OL-7313-05: The following EM attributes were added: jurisdiction information parameter (JIP), account code, authorization code, ported-in calling number, ported-in called number, calling party NP source, called party NP source, billing type (flat rate or measured rate). See EM Content, page 49. The EM billing specification reference was changed from PKT-SP-EM-I07-030815 to PKT-SP-EM-I10-040721 (Industry Standards, page 53, and throughout the document). The Cisco BTS 10200 Softswitch complies with the RKS EM billing interface requirements of PKT-SP-EM-I10-040721. Wording clarifications were made in the description of the EM billing file name (Recovering the Billing Files, page 37). The reference for EM billing file naming was changed from PKT-SP-EM-I07-030815 to EM-N-04.0186-3 (Industry Standards, page 53, and throughout the document). References to PKT-SP-EM1.5-I02-050812 were changed to PKT-SP-EM-I10-040721. Version OL-7313-04: • A link was provided to the detailed discussion of the parameters affecting the keepalive process (Provisioning the Keepalive AUEP and ICMP Ping Options, page 19). • A correction was made to the procedure to follow if checksums on the RKS do not match (Comparing Checksums, page 38). • Editorial changes were made to improve clarity and readability. Version OL-7313-03 (Release 4.5.1 only): • The privacy indicator field was added to the signaling start EM as shown in the "EM Generation Details and Content" section on page 44 section. This attribute uses the previously undefined field #12 in PKT-SP-EM1.5-I02-050812. • A new token, EM-PRIVACY-IND-SUPP, was added to CA-CONFIG table. Default=N. Version OL-7313-02: The keepalive provisioning examples (mgw-profile table) were enhanced. Version OL-7313-01: • Information was added regarding encryption of security parameters, including the Internet Key Exchange (IKE) key and Kerberos service key. • A note was added that provisioning a change in call data block (CDB) or EM billing support takes effect only after a CA switchover or restart. • The NODE token was included in media gateway (MGW) table provisioning. The originating and terminating node IDs were also included in the billing CDBs. • The billing file-naming convention (for stored EM files) was updated. • The option for billing type (flat rate or measured rate) was added in the subscriber table.

Contents

Technical Overview

This section provides technical information about the implementation of PacketCable features. It covers the following topics.

- Cisco BTS 10200 Softswitch in the PacketCable Network, page 3
- Security Interface Features, page 6
- Event Message Feature, page 8

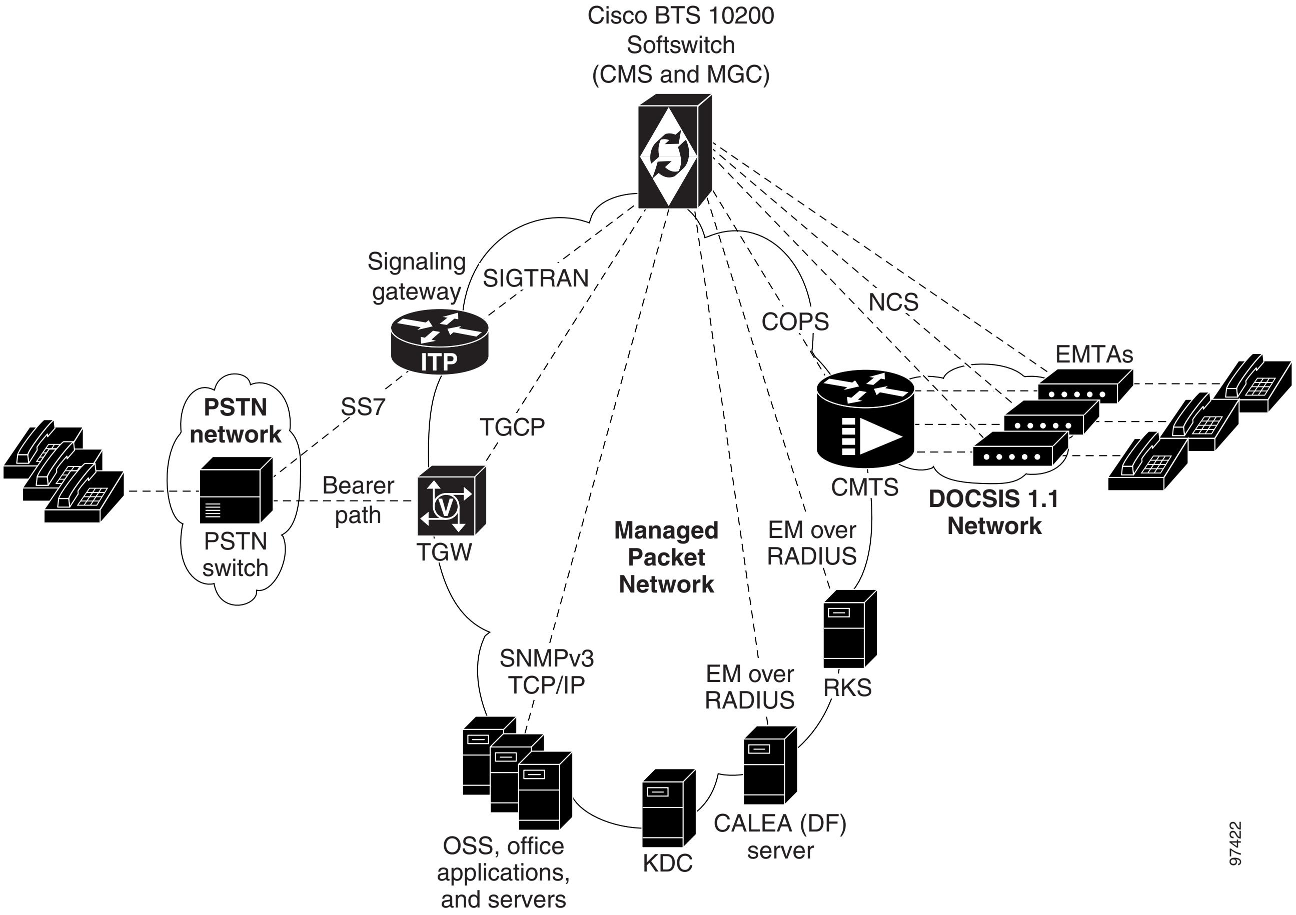
Note In this document, embedded multimedia terminal adapter (eMTA) refers to eMTAs using PacketCable Network-based Call Signaling (NCS) protocol.

Cisco BTS 10200 Softswitch in the PacketCable Network

The Cisco BTS 10200 Softswitch is a class-independent network-switching element. In a PacketCable-based network, it functions as both a call management server (CMS) and a media gateway controller (MGC). It provides call control, call routing, and signaling for several types of multimedia terminal adapters (MTAs) and embedded MTAs (eMTAs), cable modem termination systems (CMTSs), and trunking gateways (TGWs) in PacketCable-based networks. It provides interfaces to record keeping servers (RKSs) and key distribution centers (KDCs). The Cisco BTS 10200 Softswitch also communicates with announcement servers, SS7-based signaling gateways, MGCP-based media gateways (MGWs), and Session Initiation Protocol (SIP) networks.

Figure 1 shows a typical network with PacketCable-based network elements and the applicable external interfaces of the Cisco BTS 10200 Softswitch. In the PacketCable-based network, the Cisco BTS 10200 Softswitch performs the functions of both the CMS and MGC. The Cisco BTS 10200 Softswitch also provides provisionable options for customizing the external interfaces.

Figure 1 Example of PacketCable-Based Network Architecture



PacketCable-Based Interfaces

The Cisco BTS 10200 Softswitch supports signaling on specific PacketCable-based interfaces shown in Figure 1. The following list summarizes the supported protocols for each of the links:

- **CMS to MTA (NCS)**—CMS-to-MTA interface for subscriber access
- **CMS to CMTS (COPS)**—CMS-to-CMTS interface for gate management
- **CMS to RKS (EM over RADIUS)**—CMS-to-Record Keeping Server (RKS) interface for EM-based billing functions
- **MGC to RKS (EM over RADIUS)**—MGC-to-RKS interface for EM-based billing functions
- **CMS to CALEA (EM over RADIUS)**—CMS-to-CALEA server (DF) interface (Note: DF = Delivery Function)
- **MGC to TGW (TGCP)**—MGC-to-trunking gateway (TGW) interface for TGW management (which allows calls to be connected between the PacketCable network and the PSTN)

Note For a description of Cisco BTS 10200 Softswitch support for CALEA, see the *Cisco BTS 10200 Softswitch System Description*. For provisioning procedures related to CALEA support, see the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Note For information on compliance with specific paragraphs of PacketCable standards and ECNs, contact your Cisco account team.

Additional Network Interfaces

The following additional interfaces are not part of the PacketCable feature set, but they provide other important functions useful in the service provider network:

- **Cisco BTS 10200 Softswitch/Signaling Gateway (SIGTRAN)**—This interface allows calls to be made between the PacketCable network and the PSTN. The Call Agent (CA) of the Cisco BTS 10200 Softswitch interfaces to an Internet transfer point (ITP) signaling gateway (SG), for example, the Cisco 7500 series router. The ITP SG provides an SS7-based interface to the STP (PSTN).
- **MGCP Interface**—The Cisco BTS 10200 Softswitch communicates with MGCP-based TGWs that provide a bearer path to the PSTN.
- **SIP Interface**—Session Initiation Protocol (SIP) signaling is used for the following two functions:
  - Communications with another CMS
  - Access to voice mail
- **Cisco BTS 10200 Softswitch office applications (SNMPv3 and CORBA over TCP/IP)**— This interface provides communication with Operations Support System (OSS) and office applications servers.

Gate Coordination Functions

In the PacketCable environment, the Cisco BTS 10200 Softswitch performs the gate coordination functions of a CMS, including the gate controller (GC). GC signaling is based on the COPS stack. Each CMTS informs the CMS when a gate is successfully opened or closed. Two gate coordination messages are used, GATE-OPEN and GATE-CLOSE. Gate coordination is required to avoid several theft-of-service scenarios, as described in Appendix K of the *PacketCable Dynamic Quality-of-Service Specification*, PKT-SP-DQOS-I07-030815, August 15, 2003.

Note For information on compliance with specific paragraphs of PacketCable standards and ECNs, contact your Cisco account team.

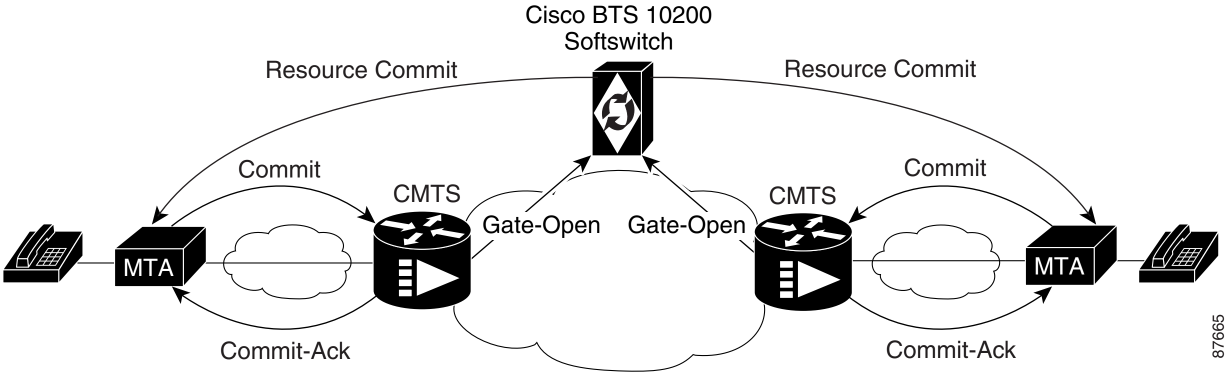
GATE-OPEN Process

The normal coordination process for GATE-OPEN signaling, illustrated in Figure 2, has four main steps:

1. During call setup, the Cisco BTS 10200 Softswitch requests the MTA to commit bearer-path resources.
2. The MTA sends a commit message to the CMTS to request opening of the gate on the bearer path.
3. The CMTS opens the gate and sends a GATE-OPEN message to the Cisco BTS 10200 Softswitch.

4. The Cisco BTS 10200 Softswitch allows the call.

Figure 2 Gate Coordination Signaling Example (GATE-OPEN)



Note If the GATE-OPEN message arrives at the Cisco BTS 10200 Softswitch before it has sent a resource-commit request to the MTA, the Cisco BTS 10200 Softswitch tears down the call.

GATE-CLOSE Process

During a call, if the Cisco BTS 10200 Softswitch receives a GATE-CLOSE message from the CMTS, it allows the call to proceed on a best-effort basis, without a guaranteed level of service. (It tears down the call only when one of the parties in the call goes on-hook.)

Security Interface Features

Note For information on compliance with specific paragraphs of PacketCable standards and ECNs, contact your Cisco account team.

The implementation of PKT-SP-SEC-I09-030728, *PacketCable Security Specification*, July 28, 2003, provides a security scheme for the voice-over-cable network built 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*, IETF (S. Kent, R. Atkinson), Internet Proposed Standard, November 1998
  - RFC 2406, *IP Encapsulating Security Payload (ESP)*, IETF (D. Piper), Internet Proposed Standard, November 1998
- IETF documents covering key management protocols—Internet Key Exchange (IKE) and Kerberos with extensions:
  - RFC 2409, *The Internet Key Exchange (IKE)*, IETF (D. Harkins, D. Carrel), Internet Proposed Standard, November 1998

  - RFC 1510, *The Kerberos Network Authentication Service (V5)*, IETF (J. Kohl, C. Neuman), September 1993, with updates presented in PKT-SP-SEC-I09-030728

The Cisco BTS 10200 Softswitch performs the security functions of a CMS and a MGC in the PacketCable environment. It supports security in accordance with PKT-SP-SEC-I09-030728 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

The system supports IPsec features for encryption and authentication on specific PacketCable-based interfaces (see Figure 1). There are two aspects to the security features, the security protocol itself (IPsec), and the key management (Kerberos or IKE). The following list summarizes the supported security type for each of the links:

- CMS to MTA (NCS)—IPsec/Kerberos
- CMS to CMTS (COPS)—IPsec/IKE
- CMS to RKS (EM over RADIUS)—IPsec/IKE
- MGC to RKS (EM over RADIUS)—IPsec/IKE
- CMS to CALEA (EM over RADIUS)—IPsec/IKE
- MGC to TGW (TGCP)—IPsec/IKE

As shown in Figure 1, there is no interface between the KDC and the Cisco BTS 10200 Softswitch. To ensure secure NCS signaling, a dynamic key exchange is performed. This exchange provides for IPsec security operations between the MTA and the Cisco BTS 10200 Softswitch. (These procedures are described in the CableLabs document *PacketCable Security Specification*, PKT-SP-SEC-I09-030728, under “Kerberized IPsec” and other sections.)

- Manual key provisioning must be used to match data stored in the KDC with data stored in the Cisco BTS 10200 Softswitch (pre-setup).
- The MTA must contact the KDC to obtain the credentials to talk to the server, which is in this case the Cisco BTS 10200 Softswitch.

Note For information on compliance with specific paragraphs of PacketCable standards and ECNs, contact your Cisco account team.

Note See the “Installation” section on page 12 regarding the requirement for setting the IPSEC_ENABLED parameter at the time of Cisco BTS 10200 Softswitch software installation.

Event Message Feature

This section describes Cisco BTS 10200 Softswitch support for the EM feature.

Billing Data Options

The Cisco BTS 10200 Softswitch can provision billing support using either of the following billing data generation methods:

- Call detail blocks (CDBs)—This is traditional post-call billing data, which is assembled into call detail records (CDRs) by an external billing mediation system or billing server.
- PacketCable event messages (EMs)—This is real-time call data flow, which is transferred to an external Record Keeping Server (RKS) that assembles CDRs from the EMs.

The Cisco BTS 10200 Softswitch should be provisioned to generate either EMs or CDBs, *but not both*.

Caution We strongly recommend that you provision the Cisco BTS 10200 Softswitch to generate either EMs or CDBs, but not both. Attempting to generate both types of records simultaneously can significantly degrade system performance. See the "Provisioning the System to Generate EMs for Billing" section on page 33 for provisioning details.

Note The content of the CDBs is outside the scope of this document. See the *Cisco BTS 10200 Softswitch Billing Interface Guide* for information about CDBs.

Description of the Event Message Feature

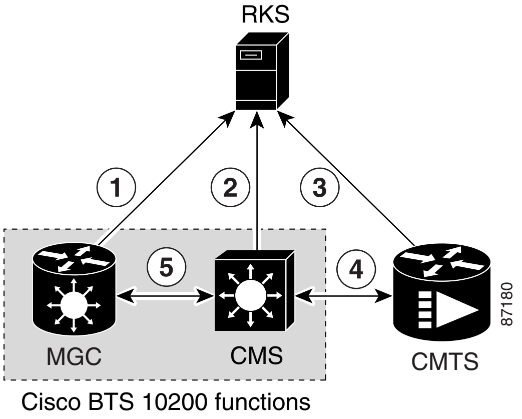
EMs are real-time data records containing information about network usage and activities. (They must not be confused with system event messages that report events and sometimes trigger alarms.) EMs are used in PacketCable networks to collect resource usage data for billing purposes. In the PacketCable architecture, EM generation is based on the half-call model. A single EM can contain complete usage data or it might contain only part of the usage information.

The Record Keeping Server (RKS) is a PacketCable network element that receives EMs from network elements, such as the call management server (CMS), media gateway controller (MGC), and the cable modem termination system (CMTS). The physical Cisco BTS 10200 Softswitch contains both CMS and MGC logical network elements. The EMs generated by both the CMS and MGC are sent to the RKS. The RKS correlates the information in multiple EMs and provides the complete record of service for a call, which is referred to as a CDR.

Note For information about EM-related operations on the Cisco BTS 10200 Softswitch, see the "Operations, Billing, and EM Transfer Procedures" section on page 36.

Figure 3 illustrates the PacketCable network elements that are involved in the EM process.

Figure 3 Event Message Interfaces



The EM related interfaces illustrated here are described as follows:

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

PacketCable EMs can support billing and settlement activities for single-zone architectures. The originating and terminating CMSs exchange unique Billing Correlation IDs (BCIDs) and Financial Entity IDs (FEIDs) for each half of the call. The originating CMS sends a BCID and an FEID in the INVITE message. The Cisco BTS 10200 Softswitch allocates the BCID for calls it originates or terminates. Along with the FEID, the BCID is used across network elements to reference calls. The FEID is provisioned on a system-wide basis (a single setting for the Cisco BTS 10200 Softswitch) as defined in the "Provisioning the System to Generate EMs for Billing" section on page 33.

Event Message Generation Details and Content

See the "EM Generation Details and Content" section on page 44 for information on EM data.

Timestamp Support for Event Messages

The system-generated timestamps for EMs are based on the host operating system (OS) time and time zone. This data is not affected by CLI provisioning. The Solaris OS obtains the time automatically through Network Time Protocol (NTP) services.

Caution Users should never attempt to modify the system date or time in a Cisco BTS 10200 Softswitch host machine while system components (CA, FS, EMS, and BDMS) are running. The attempt could cause the system to have serious problems. Allow the Solaris OS to obtain the time automatically through NTP services.

Event Message Transport

The RADIUS transport protocol is used between the Cisco BTS 10200 Softswitch (CMS/MGC) and the RKS. The system sends EMs to an RKS without waiting for acknowledgment of the previous message. The maximum number of pending ACK messages is 256.

EMs are first sent to the primary RKS. If the specified number of retry attempts fail, the EMs are sent to the secondary RKS. If one RKS is found to be unreachable, then the other RKS is considered for subsequent messages. If both the primary and secondary RKSs become unreachable, the EMs are stored in an error file on the hard disk (as described in the "Event Message Storage on the CA" section on page 10) and a timer is started. When the timer expires, newly arriving EMs are sent to the primary RKS.

Note If EMs are being sent to the primary RKS and the primary RKS goes down, the Cisco BTS 10200 Softswitch sends subsequent EMs to the secondary RKS. When the primary RKS comes back up, the Cisco BTS 10200 Softswitch continues to send EMs to the secondary RKS. (It does not automatically begin sending them to the primary RKS.) Provisioning of timers and retry attempts is described in the "Provisioning Support for EM Transmission and Storage" section on page 31.

Note Remote Access Dial-In User Service (RADIUS) is a client/server protocol used for Authorization, Authentication, and Accounting (AAA). The RADIUS protocol is an industry standard for remote access AAA defined in a set of Internet Engineering Task Force (IETF) standards: RFC 2865 and RFC 2866.

Event Message Storage on the CA

Note For information on compliance with specific paragraphs of PacketCable standards and ECNs listed in this document, contact your Cisco account team.

EMs are stored in the network element (CA) that generates them until they are transferred to the RKS. After receipt of the EMs is acknowledged by the RKS, they are deleted. The number of EMs generated by the Cisco BTS 10200 Softswitch depends on the number of calls processed. Multiple EMs are generated for each call. Depending on provisioning in the call-agent-profile table and the type of call, EMs can be generated by the CMS or MGC (or both) within the CA. The exact storage requirement varies depending on the rate of EM generation and how long the Cisco BTS 10200 Softswitch is required to keep the records before transferring them to an RKS.

The Cisco BTS 10200 Softswitch generates and stores EMs with the following characteristics:

- EMs are generated in real time during a call. EMs contain timestamps with a granularity of 1 millisecond. The time interval between generation and transmission is not specified.
- The Cisco BTS 10200 Softswitch synchronizes with the network clock using NTP at least once per hour. The deviation of the clock in the Cisco BTS 10200 Softswitch remains within ±100 milliseconds between NTP synchronizations.

- EMs that cannot be successfully transferred to the RKS due to loss of communication are stored in the /opt/BTSem directory on the CA. The system uses the file-naming conventions specified in PacketCable ECN EM-N-04.0186-3 for the stored EMs. The maximum EM file size and the time limit on keeping a file open are provisionable, as described in the "Provisioning Support for EM Transmission and Storage" section on page 31. These files are not automatically deleted or transferred out of the CA.

Caution Event messages that cannot be successfully transferred to the RKS due to loss of communication are not automatically deleted or transferred out of the CA. *You must transfer these files to the RKS when communication is restored.*

The procedure for doing this is provided in the "Manual Recovery and Transfer of Stored EMs" section on page 36.

- Each time an EM file is placed in local storage, the system checks current disk usage and takes the following actions:
  - The system generates an alarm if the disk space allocated to EMs fills up to a certain level—50 percent (minor alarm), 70 percent (major alarm), or 100 percent (critical alarm).
  - When the critical condition is reached, the system issues a critical alarm, and further EMs are dropped without any additional warning.
  - When the critical condition is reached, the disk usage is monitored periodically (one time every minute) to check if disk space usage has decreased and EMs can be stored again.

Planning

Delivery of the features and functions described in this document requires interoperability with the network elements connected to the Cisco BTS 10200 Softswitch. See the "Component Interoperability" section in the *Cisco BTS 10200 Softswitch Release Notes*, which lists the specific peripheral platforms, functions, and software loads that have been tested by Cisco for interoperability with the Cisco BTS 10200 Softswitch.

Note The "Component Interoperability" section in the *Cisco BTS 10200 Softswitch Release Notes* is intended as a guide. Earlier or later releases of platform software might be interoperable, and it might be possible to use other functions on these platforms. The list certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the Cisco BTS 10200 Softswitch.

Installation

Installation of Cisco BTS 10200 Softswitch software follows a standard process. For details, see the *Application Installation Procedure* in the Cisco BTS 10200 Softswitch documentation set. Of the three main PacketCable feature areas (DQoS, EM, and security), two of them (DQoS and EM) are always installed, and do not require the setting of any special flags during software installation. However, the third area (security) is not installed unless a special flag (IPSEC_ENABLED) is set in the opticall.cfg file during software installation.

Caution We strongly recommend that you contact Cisco TAC if you believe that you might need to reinstall Cisco BTS 10200 Softswitch software in order to change the value of IPSEC_ENABLED.

Provisioning Procedures

This section explains how to perform the following procedures:

- Provisioning Basic PacketCable and DQoS Features, page 12
- Provisioning Security Interfaces, page 22
- Provisioning Event Messages, page 31

Tip These tasks include examples of CLI commands that illustrate how to provision the specific feature. Most of these tables have additional tokens that are not included in the examples. For a complete list of all CLI tables, tokens, descriptions, valid ranges, and default values, see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

Note The command sequences shown in this section provide guidance on how to provision a new system. Therefore, in most cases the commands are “add” commands. If you are modifying previously provisioned GWs, TGs, and so forth, use the “change” commands.

Provisioning Basic PacketCable and DQoS Features

This section describes how to provision the Cisco BTS 10200 Softswitch interfaces to connect to other PacketCable-based NEs and how to select dynamic quality of service (DQoS) options. It includes the following tasks:

- Provisioning CMS Parameters, page 13
- Provisioning the CMS Interfaces to the CMTS and eMTA, page 15
- Provisioning DQoS Parameters for Codec Negotiation Service, page 18
- Provisioning TGCP Interfaces to TGWs, page 18
- Provisioning the Keepalive AUEP and ICMP Ping Options, page 19

Provisioning CMS Parameters

This section describes how to provision DQoS functionality for the CMS logical entity on the Cisco BTS 10200 Softswitch (Call Agent).

SUMMARY STEPS

1. Enable DQoS support—**change call-agent-profile**.
2. Set CMS timers in Call Agent Configuration (ca-config) table (optional, if using other than the default values)—**change ca-config**.
3. Set the local ringback flag, differential service code point (DSCP)/type of service (TOS) parameter, and maximum MGCP datagram sizes in the ca-config table (optional, if using other than the default values)—**change ca-config**.

Note The token values shown in this section are examples.

DETAILED STEPS

	Command Examples	Purpose
Step 1	`change call-agent-profile id=CA146; dqos-supp=y; description=BostonCA33`	Enables DQoS support. **Tip** The command is shown as **change call-agent-profile**. However, if the system responds that the call-agent-profile ID does not exist, reenter the command as **add call-agent-profile**.

Step 2	`CHANGE CA-CONFIG TYPE=DQOS-T1-TIMER; DATATYPE=INTEGER; VALUE=250;`
	`CHANGE CA-CONFIG TYPE=DQOS-DS-SLACK-TERM; DATATYPE=INTEGER; VALUE=30000;`
	`CHANGE CA-CONFIG TYPE=DQOS-GATE-TIMER; DATATYPE=INTEGER; VALUE=3;`
		Specifies values other than the defaults for individual CMS timers in the ca-config table. The applicable timers are DQOS-T1-TIMER, DQOS-T5-TIMER, DQOS-T7-TIMER, DQOS-T8-TIMER, DQOS-DS-SLACK-TERM, DQOS-US-SLACK-TERM, and DQOS-GATE-TIMER.
		Tip The default values for these timers might be adequate for your specific case. In each case, you can use the **show** command to find out how the parameter is currently set. See the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for parameter definitions and valid ranges.
		Tip The command is shown as **change ca-config**. However, if the system responds that the parameter does not exist, reenter the command as **add ca-config**.

	Command Examples	Purpose

Step 3	`CHANGE CA-CONFIG TYPE=LOCAL-RINGBACK; DATATYPE=BOOLEAN; VALUE=N;`
	`CHANGE CA-CONFIG TYPE=COPS-DSCP-TOS; DATATYPE=INTEGER; VALUE=240;`
	`CHANGE CA-CONFIG TYPE=MAX-MGCP-DATAGRAM; DATATYPE=INTEGER; VALUE=3900;`
		Specifies additional ca-config parameters that can be set to values other than the defaults.
		Tip The default values for these parameters might be adequate for your specific case. In each case, you can use the **show** command to find out how the parameter is currently set. See the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for parameter definitions and valid ranges.
		Note The MAX-MGCP-DATAGRAM parameter specifies the maximum size of an MGCP message datagram (which can include one or more piggybacked messages) that the Cisco BTS 10200 Softswitch can decode before discarding the rest of the message part. The default value of 4000 bytes is adequate for most applications, and *Cisco does not recommend that you change this value* unless you are deploying MGCP-based media gateways or MTAs that require larger datagram sizes.
		Tip The command is shown as **change ca-config**. However, if the system responds that the parameter does not exist, reenter the command as **add ca-config**.

Provisioning the CMS Interfaces to the CMTS and eMTA

This section describes how to provision the interfaces to the CMTS and eMTA nodes. Specific tables are provisioned for each of these interfaces:

- **CMTS**—The Aggregation (aggr) table defines the parameters for the connected CMTS devices. These parameters are used by the COPS adapter to establish and terminate TCP connections to the CMTS.
- **MTA (or eMTA)**—The Cisco BTS 10200 Softswitch uses the Media Gateway Profile (mgw-profile), mgw, and termination tables to establish and terminate connections to the eMTAs. The supported MGCP variant is NCS. The following tables are provisioned for this interface:
  - The mgw-profile table provides templates for defining each type of eMTA by hardware vendor. It identifies the specifications and settings necessary for communications between the Cisco BTS 10200 Softswitch (which functions as the CMS) and each type of eMTA. An mgw-profile ID must be created in this table before entries can be added to the mgw table. Several tokens have values that can be overwritten after the Cisco BTS 10200 Softswitch (CMS) queries the eMTA for supported capabilities. If the eMTA returns a value different from the value originally provisioned in the Cisco BTS 10200 Softswitch, the returned value automatically replaces the originally provisioned value.
  - The mgw table holds information about each eMTA managed by the Cisco BTS 10200 Softswitch (CMS). The eMTA can be uniquely addressed by domain name, an IP address, or the TSAP address.
  - The termination table holds information about each endpoint in eMTAs managed by the CMS. Termination events and signals are grouped into packages, which are groupings of events and signals supported by a particular type of endpoint, such as an eMTA endpoint. One or more packages can exist for a given endpoint-type.

SUMMARY STEPS

1. Create the CMTS and enable DQoS support—**add aggr**.
2. Create the profile for eMTA and specify the appropriate parameters—**add mgw-profile**.
3. Verify that all parameters affecting eMTAs are properly populated, either by default or by the operator—**show mgw-profile**.
4. Modify parameters affecting eMTAs, if necessary—**change mgw-profile**.
5. Create the specific eMTA, associate it with the applicable CMTS, and set appropriate parameters—**add mgw**.
6. Add the line termination for an eMTA—**add termination**.
7. Bring the eMTA into service—**control mgw**.
8. Equip the termination and place it in service— **equip subscriber-termination** and **control subscriber-termination**.

Note The token values shown in this section are examples.

DETAILED STEPS

	Command Examples	Purpose

Step 1	**add aggr id=*cmts777*;**
	tsap-addr=ADDRESS123.cisco.com;
	dqos-supp=Y;
		Creates the CMTS (aggregation device) and enables DQoS support.
		Note The TSAP-ADDR can be a DNS or IP address. If you enter a DNS address, it must be a fully qualified domain name (FQDN).
		Caution DQoS is disabled (DQOS-SUPP=N) by default. Set this value to Y to enable DQoS.

Step 2	**add mgw-profile id=mgwprofile777;**
	mgcp-version=MGCP-1-0; mgcp-variant=NCS-1-0;
	mgcp-default-pkg=LINE;
	mgcp-conn-id-at-gw-supp=n;
		Creates the mgw-profile for this type of eMTA, and specifies values for the optional parameters.
		Tip The default values for these parameters might be adequate for your specific case. In each case, you can use the **show** command to find out how the parameter is currently set. See the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for parameter definitions and valid ranges.

Step 3	**show mgw-profile id=mgwprofile777;**
	Verify that the following values are present:
	vendor=Cisco [or applicable vendor name]
	mgcp-version=MGCP-1-0
	mgcp-variant=NCS-1-0
	mgcp-default-pkg=LINE
	codec-neg-supp=y
	pc-mptime-supp=y
	mgcp-xdlcx-supp=n
	domain-name-caching-supp=y
	mgcp-conn-id-at-gw-supp=y
		Shows the provisioned values for the parameters in the mgw-profile table.

Step 4	**change mgw-profile id=mgwprofile777;**
	mgcp-version=MGCP-1-0; mgcp-variant=NCS-1-0;
		If any of the mgw-profile token values (from Step 3) need to be changed, use the **change mgw-profile** command.

	Command Examples	Purpose
Step 5	`add mgw id=CiscoGW50; tsap-addr=192.168.26.104; call-agent-id=CA146; mgw-profile-id=mgwprofile777; type=rgw; aggr-id=cmts777; node=main0044;`	Creates the MGW ID for a single eMTA, and specifies values for the other required parameters. **Note** Be sure to set TYPE=RGW for an eMTA. **Note** You must enter the value for AGGR-ID to identify the appropriate CMTS for this eMTA. **Note** The **node** token allows you to identify a hybrid fiber coax (HFC) node to which the eMTA is assigned. Typically, each eMTA is assigned to a node, and one or more nodes are assigned to a CMTS.
Step 6	`add termination prefix=aaln/; port-start=1; port-end=2; type=LINE; mgw-id=CiscoGW50;`	Creates the line termination for the eMTA and specifies values for the required parameters. **Note** For eMTA terminations, always enter TYPE=LINE.

Step 7	`CONTROL MGW ID=CiscoGW50; TARGET-STATE=INS; MODE=FORCED;`
	`STATUS MGW ID=CiscoGW50;`
		Brings the eMTA in service (INS state), and verifies that the administrative state is INS.

Step 8	`EQUIP SUBSCRIBER-TERMINATION ID=sub3456;`
	`CONTROL SUBSCRIBER TERMINATION ID=sub3456; TARGET-STATE=INS; MODE=FORCED;`
	`STATUS SUBSCRIBER TERMINATION ID=sub3456;`
		Equips the termination, places it in service (INS state), and verifies that the administrative state is INS.

Provisioning DQoS Parameters for Codec Negotiation Service

The Quality of Service (qos) table is used in providing the codec negotiation service. Codec negotiation is the process the Cisco BTS 10200 Softswitch uses to find a common codec for the compression or decompression of a signal between two gateways. The Subscriber Profile (subscriber-profile) and Subscriber (subscriber) tables point to the qos table.

The following commands allow you to specify the required characteristics for these tables.

SUMMARY STEPS

1. Provision QOS parameters—**add qos**.
2. Assign a specific QOS to each subscriber-profile or subscriber—
add subscriber-profile; **add subscriber**.

Note The token values shown in this section are examples.

DETAILED STEPS

	Command Examples	Purpose
Step 1	**`add qos id=Gold1; codec-type=PCMU;`**	Adds a qos with the preferred codec type and other parameters.

Step 2	**`add subscriber-profile id=NorthDallas; dial-plan-id=dp1; POP=BLDG222; qos-id=Gold1;`**
	`add subscriber id=Person29; dn1=800-555-0029; sub-profile-id=richardson;`
	`add subscriber id=Person123; dn1=800-555-0123; sub-profile-id=richardson; qos-id=Gold1;`
		Assigns a qos ID to each subscriber-profile and/or subscriber.

Provisioning TGCP Interfaces to TGWs

This section describes how to provision the TGCP interfaces to the TGWs.

The mgw-profile table provides templates for defining each type of TGW by hardware vendor. It identifies the specifications and settings necessary for communications between the Cisco BTS 10200 Softswitch (which functions as the MGC) and each type of TGW. Several tokens in this table have values that can be overwritten after the Cisco BTS 10200 Softswitch (MGC) queries the TGW for supported capabilities. If the TGW returns a value different from the value originally provisioned in the Cisco BTS 10200 Softswitch, the returned value automatically replaces the originally provisioned value.

SUMMARY STEPS

1. Enable TGCP support for each type of TGW—**add mgw-profile**.
2. Link each TGW to an mgw-profile—**add mgw**.
3. Add the trunk termination for a TGW—**add termination**.
4. Provision QOS parameters—**add qos**.
5. Assign a QOS-ID to the TGW—**add trunk-grp**.

Note The token values shown in this section are examples.

DETAILED STEPS

	Command Examples	Purpose
Step 1	**`add mgw-profile id=tgwprf222; vendor=cisco; mgw-type=MGX8850; mgcp-version=MGCP-1-0; mgcp-variant=TGCP-1-0; mgcp-default-pkg=TRUNK; pc-mptime-supp=y;`**	Creates an mgw-profile for this type of TGW and specifies values for required parameters. **Note** For most TGWs, set PC-MPTIME-SUPP to Y. However, for a Cisco MGX8850 VISM gateway, the MP function is not available. Therefore, set the PC-MPTIME-SUPP token to N for a Cisco MGX8850 VISM gateway. **Note** Be sure to set the following values for a TGW: MGCP-VERSION=MGCP-1-0 MGCP-VARIANT=TGCP-1-0 MGCP-DEFAULT-PKG=TRUNK
Step 2	**`add mgw id=tgw50; tsap-addr=TGW1515.cisco.com; call-agent-id=CA146; mgw-profile-id=tgwprf222; type=tgw;`**	Links a specific TGW to the applicable mgw-profile. **Note** Be sure to set TYPE=TGW.
Step 3	**`add termination prefix=S0/ds1-2/; mgw-id=tgw50; port-start=1; port-end=24; type=TRUNK;`**	Creates trunk terminations for the TGW. **Note** Be sure to set TYPE=TRUNK.
Step 4	**`add qos id=gold-service; lptime=20; hptime=20; codec-type=PCMU;`**	Adds a qos with the preferred codec type and other parameters.
Step 5	**`add trunk-grp id=101; call-agent-id=CA146; tg-type=ss7; qos-id=gold-service; mgcp-pkg-type=IT;`**	Assigns a qos ID to each TRUNK-GRP. **Note** For trunk groups on TGCP-based TGWs (MGCP-VARIANT=TGCP-1-0 in the mgw-profile table), set the MGCP-PKG-TYPE value to IT (ISUP trunk package).

Provisioning the Keepalive AUEP and ICMP Ping Options

This section explains how to provision the keepalive AUEP and ICMP ping options. There are two tokens to provision:

- AUEP and ICMP pings can be globally disabled on the system by use of the mgw-monitoring-enabled token in the Call Agent (call-agent) table.
- If globally enabled in the call-agent table, these pings can be selectively enabled or disabled for each mgw-profile by use of the keepalive-method token in the mgw-profile table. Each MGW (eMTA) is linked to an mgw-profile by means of the mgw table.

SUMMARY STEPS

1. Show the setting for mgw-monitoring-enabled—**show call-agent**.
2. If necessary, change the value of mgw-monitoring-enabled—**change call-agent**.
3. Show the setting for keepalive-method—**show mgw-profile**.
4. If necessary, change the value of keepalive-method—**change mgw-profile**.
5. If necessary, change the value of other keepalive tokens—**change mgw-profile**.
6. Link individual MGWs (eMTAs) to MGW profiles—**add mgw**.

Note If mgw-monitoring-enabled=Y (the default value) in the call-agent table, the system checks the provisioning of the keepalive-method token in the mgw-profile table for each MGW.

However, if mgw-monitoring-enabled=N, the AUEP and the ICMP ping are globally disabled, and the keepalive-method token is not checked.

Note The token values shown in this section are examples. In addition, these tables have many additional optional tokens not shown in these examples. For a complete list of all the tokens for each table, see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

DETAILED STEPS

	Command Examples	Purpose
Step 1	**`SHOW CALL-AGENT ID=CA146;`** The system responds with the current settings for the call-agent table. The default value of MGW-MONITORING-ENABLED is Y.	Show the setting for mgw-monitoring-enabled in the call-agent table.

Step 2	**`change call-agent id=CA146;`**
	`tsap-addr=CA146.cisco.com;`
	`mgw-monitoring-enabled=Y;`
		If the current value of mgw-monitoring-enabled is N, use this command to change it to Y. (Otherwise, go to Step 3.)

Step 3	**`show mgw-profile id=mgwprofile001;`** The system responds with the current settings for the mgw-profile table.	Show the setting for keepalive-method in the mgw-profile table.

Step 4	**`change mgw-profile id=mgwprofile001;`**
	`keepalive-method=<value (see options)>;`
	`change mgw-profile id=mgwprofile001;`
	`keepalive-method=auep-icmp;`
		If necessary, change the value of keepalive-method in the mgw-profile table.
		The options for keepalive-method are:
		• none—Disable both AUEP and ICMP ping.
		• auep—Enable AUEP ping but not ICMP ping (this is the default value).
		• auep-icmp—Enable sending of an AUEP ping followed (if AUEP is unsuccessful) with an ICMP ping.

	Command Examples	Purpose
Step 5	**`change mgw-profile id=mgwprofile001; mgcp-keepalive-interval=120; mgcp-keepalive-retries=4; mgcp-max-keepalive-interval=720; mgcp-max1-retries=3; mgcp-max2-retries=4;`**	If necessary, change the value of other keepalive tokens in the mgw-profile table. **Note** The mgcp-max1-retries and mgcp-max2-retries tokens can be adjusted, if necessary, to improve response if there are network bandwidth or reliability issues, or if an MGW is slow in responding to commands from the CA. For a detailed explanation of how these and other parameters affect the keepalive process, see Appendix C of the *Cisco BTS 10200 Softswitch Troubleshooting Guide.*
Step 6	**`add mgw id=mgw_abc; mgw-profile-id=mgwprofile001;`**	Links an individual MGW (eMTA) to an mgw-profile.

Provisioning Security Interfaces

This section describes the PacketCable-based security interface feature and explains how to provision security options. The subsections are as follows:

- Provisioning Parameters for Secured Media, page 22
- Provisioning Security Interfaces to the MTA, page 23
- Provisioning Security Interfaces to the CMTS, page 26
- Provisioning Security Interfaces to the TGW, page 27
- Provisioning Security Interfaces to the RKS, page 28
- Provisioning IPsec Security Associations and Ciphersuite Algorithms, page 29

Note A global security parameter, IPSEC_ENABLED, must already be set in the initial configuration file (opticall.cfg) during the Cisco BTS 10200 Softswitch software installation process. This parameter enables or disables the IPsec feature on the Cisco BTS 10200 Softswitch. See the detailed requirement in the "Installation" section on page 12.

Provisioning Parameters for Secured Media

This section describes how to provision the SECURED-MEDIA-ONLY flag, which affects transmission of security parameters from the qos and ciphersuite tables when the system sets up a call. This parameter affects the setup of calls to unsecured MGWs.

SUMMARY STEPS

1. Show the current setting of the SECURED-MEDIA-ONLY flag—**show ca-config**.
2. If necessary, change the value of the SECURED-MEDIA-ONLY flag—**change ca-config**.

DETAILED STEPS

	Command Examples	Purpose
Step 1	`SHOW CA-CONFIG TYPE=SECURED-MEDIA-ONLY;`	Displays the current setting of the secured-media-only flag: • If set to Y, the Cisco BTS 10200 Softswitch forces the security parameters from the qos and ciphersuite tables to the endpoint when it sets up the connection. This may result in call failure if either side cannot handle these parameters. • If set to N, the Cisco BTS 10200 Softswitch forces the security parameters from the qos and ciphersuite tables when it sets up the connection to the endpoint *only if* both sides can handle the security parameters.
Step 2	`CHANGE CA-CONFIG TYPE=SECURED-MEDIA-ONLY; DATATYPE=BOOLEAN; VALUE=Y;`	If necessary, change the setting of the secured-media-only flag. **Caution** Do not change this value unless specified by your network administrator. This command can affect the setup of calls to unsecured MTAs. **Tip** The command is shown as **change ca-config**. However, if the system responds that the parameter does not exist, reenter the command as **add ca-config**.

Provisioning Security Interfaces to the MTA

The MTA is the only device that uses Kerberos key management. This section explains how to provision the MTA IP security (IPsec) interface, including:

- Provisioning Kerberos
- Provisioning IPsec policy
- Enabling IPsec

Note The token values shown in this section are examples. For detailed token descriptions, see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

SUMMARY STEPS

1. Provision Kerberos parameters—**add ipsec-kerberos**.
2. Display the rolling list of old Kerberos service keys—**show ipsec-kerberos-keys** (optional).
3. Add an IPsec policy for all incoming and outgoing traffic on the MTA—**add ipsec-policy**.
4. Enter values for additional security parameters—**change mgw-profile** (optional).

DETAILED STEPS

	Command Examples	Purpose
Step 1	`add ipsec-kerberos krb-fqdn=cms-ca1.ciscolab.com; krb-realm=cisco-realm.com; krb-srv-key=546869732069732061206b6579206f6620 3234206368612e; srv-key-version=8;`	Provisions Kerberos parameters. **Note** The KRB-FQDN must be the FQDN used on the KDC for this node. KRB-REALM is used to create the CMS principal name. If the krb-serv-key is changed, the srv-key-version must also be changed, and if the srv-key-version is changed, the krb-srv-key must also be changed. Neither krb-srv-key nor srv-key-version, can already exist in the ipsec-kerberos-keys table. The system updates the ipsec-kerberos table before it updates the ipsec-kerberos-keys table. **Note** After you enter a value for the krb-srv-key parameter, the system encrypts it and stores the encrypted value. A **show ipsec-kerberos** command displays the encrypted value only. There is no way to display the value of the krb-srv-key that you originally entered.
Step 2	`SHOW IPSEC-KERBEROS-KEYS;`	Displays the rolling list of old Kerberos service keys. **Note** This step is optional. Use this command when you need to display the list.
Step 3	`ADD IPSEC-POLICY;` See substeps a. and b. below.	Adds an IPsec policy for all incoming and outgoing traffic on the MTA. Perform one or more of the following steps, as applicable: • Full-duplex security policy – Using FQDN – Using IP addresses • Half-duplex security policy

	Command Examples	Purpose

a.	Provisioning example using FQDNs:
	Use these two commands (examples shown):
	`add ipsec-policy id=mta01-out;`
	`src-fqdn=cms-ca1.ciscolab.com;`
	`dest-fqdn=mta1.ciscolab.com; action=apply;`
	
	`add ipsec-policy id=mta01-in;`
	`src-fqdn=mta1.ciscolab.com;`
	`dest-fqdn=cms-ca1.ciscolab.com; action=permit;`
	
	Alternatively, use this one command (example shown):
	`add ipsec-policy id=mta01;`
	`src-fqdn=cms-ca1.ciscolab.com;`
	`dest-fqdn=mta1.ciscolab.com; action=ipsec`
	
	Provisioning example using IP addresses:
	Use these two commands (examples shown):
	`add ipsec-policy id=mta02-out;`
	`src_ipaddr=192.168.45.211;`
	`src_ipmask=255.255.255.0;`
	`dest_ipaddr=192.168.17.222; action=apply;`
	
	`add ipsec-policy id=mta02-in;`
	`src_ipaddr=192.168.45.211;`
	`src_ipmask=255.255.255.0;`
	`dest_ipaddr=192.168.17.222; action=permit;`
	
	Alternatively, use this one command (example shown):
	`add ipsec-policy id=mta02;`
	`src_ipaddr=192.168.45.211;`
	`src_ipmask=255.255.255.0;`
	`dest_ipaddr=192.168.17.222; action=ipsec`
		Full-duplex security policy—When the MTA vendor applies security policy on all ports, use action=apply for outbound traffic and action=permit for inbound traffic. Alternatively, you can use a single command with action=ipsec for all outbound and inbound traffic.
		
		Caution You must specify at least one of the following: src-fqdn, src-ipaddr, or src-port.
		You must also specify at least one of the following: dest-fqdn, dest-ipaddr, or dest-port.
		
		The value of the ***action*** token defines whether security is applied to outbound or inbound traffic, both, or neither. This is a mandatory token. The allowed values are:
		• PERMIT—Security on inbound traffic
		• APPLY—Security on outbound traffic
		• IPSEC—Security on both inbound and outbound traffic
		• BYPASS—No security

b.	Use these two commands (examples shown):
	`add ipsec-policy id=mta01-out;`
	`src-fqdn=cms-ca1.ciscolab.com;`
	`dest-fqdn=mta1.ciscolab.com; action=apply;`
	
	`add ipsec-policy id=mta01-in;`
	`src-fqdn=mta1.ciscolab.com;`
	`dest-fqdn=cms-ca1.ciscolab.com; action=permit;`
	`dest-port=2727;`
		Half-duplex security policy—When the MTA vendor applies security policy on a specific signaling port only, use action=apply for outbound traffic and action=permit and dest-port=<destination port> for inbound traffic.

	Command Examples	Purpose

Step 4	**change mgw-profile id=cvmdqos;**
	krb-reest-flag=[y|n];
	ipsec-sa-esp-cs=[cipher suite for ESP];
	ipsec-sa-lifetime=[IPsec SA expiration time];
	ipsec-sa-grace-period=[expiration grace period];
	ipsec-ulp-name=[IP | UDP | TCP];
	ike-group=[1|2];
	ike-sa-lifetime=[IKE SA expiration time];
	ike-cs=[cipher suite for IKE];
	ike-key=[IKE pre-shared key];
		Enters values for additional security parameters.
		Note This step is optional. Use this command only if you need to modify these values in your system.
		Tip The default values of these security parameters are sufficient for some networks. Before making any changes, you can use the **show** command to determine if changes are needed to any of the default values.
		Note After you enter a value for the ike-key parameter, the system encrypts it and stores the encrypted value. A **show mgw-profile** command displays the encrypted value only. There is no way to display the value of the ike-key that you originally entered.

Provisioning Security Interfaces to the CMTS

This section explains how to provision security interfaces to the CMTS.

SUMMARY STEPS

1. Add a security policy for the CMTS—**add ipsec-policy**.
2. Enables IPsec for the CMTS—**change aggr**.
3. Enter values for additional security parameters for this CMTS—**change aggr** (optional).

Note The token values shown in this section are examples.

DETAILED STEPS

	Command Examples	Purpose

Step 1	**add ipsec-policy id=cmts01;
	src-fqdn=cms-ca1.ciscolab.com;
	dest-fqdn=cmts1.ciscolab.com; action=ipsec;**
		Adds a security policy for the CMTS.

Step 2	**change aggr id=cmts1;
	tsap-addr=[DNS/*IP-address*]; ike-key=<IKE preshared security key>;**
		Enables IPsec for the CMTS.
		Note After you enter a value for the ike-key parameter, the system encrypts it and stores the encrypted value. A **show aggr** command displays the encrypted value only. There is no way to display the value of the ike-key that you originally entered.

Step 3	**change aggr id=cmts1;
	tsap-addr=[DNS/*IP-address*];
	ipsec-sa-esp-cs=[cipher suite for ESP];
	ipsec-sa-lifetime=[IPsec SA expiration time];
	ipsec-sa-grace-period=[expiration grace period]; ipsec-ulp-name=[IPsec SA upper layer protocol]; ike-group=[1|2];
	ike-sa-lifetime=[IKE SA expiration time];
	ike-cs=[cipher suite for IKE]; ike-key=234;
	description=CMTS_City1;**
		Enters values for additional security parameters for this CMTS.
		Note This step is optional. Use this command only if you need to modify these values in your system.
		Tip The default values of these security parameters are sufficient for some networks. Before making any changes, you can use the **show** command to determine if changes are needed to any of the default values.
		Note The **aggr id** and **tsap-addr** are both required in this command.

Provisioning Security Interfaces to the TGW

This section explains how to provision security interfaces to the TGW.

SUMMARY STEPS

1. Add a security policy for the TGW—**add ipsec-policy**.
2. Enable IPsec for the TGW—**change mgw-profile**.
3. Enter values for additional security parameters for this TGW—**change mgw-profile** (optional).

Note The token values shown in this section are examples.

DETAILED STEPS

<table>
<tr><th></th><th>Command Examples</th><th>Purpose</th></tr>
<tr><td>Step 1</td><td><code>add ipsec-policy id=tgw01; src-fqdn=cms-ca1.ciscolab.com; dest-fqdn=tgw1.ciscolab.com; action=ipsec;</code></td><td>Adds a security policy for the TGW.
Note You must specify at least one source (src-fqdn, src-ipaddr, or src-port), and at least one destination (dest-fqdn, dest-ipaddr, or dest-port).
Note You cannot specify both a SRC-FQDN and a SRC-IPADDR at the same time. You cannot specify both a DEST-FQDN and a DEST-IPADDR at the same time.</td></tr>
<tr><td>Step 2</td><td><code>change mgw-profile id=tgw1; ike-key=<IKE preshared security key>;</code></td><td>Enables IPsec for the TGW—To enable IPsec on the TGW, change the mgw-profile entry associated with this TGW.
Note Changing this entry enables security for all TGWs that use this profile, so you might want to have a security-enabled and security-disabled profile for each vendor class.
Note After you enter a value for the ike-key parameter, the system encrypts it and stores the encrypted value. A <b>show mgw-profile</b> command displays the encrypted value only. There is no way to display the value of the ike-key that you originally entered.</td></tr>
<tr><td>Step 3</td><td><code>change mgw-profile id=cvmdqos; krb-reest-flag=[y|n]; ipsec-sa-esp-cs=[cipher suite for ESP]; ipsec-sa-lifetime=[IPsec SA expiration time]; ipsec-sa-grace-period=[expiration grace period]; ipsec-ulp-name=[IP | UDP | TCP]; ike-group=[1|2]; ike-sa-lifetime=[IKE SA expiration time]; ike-cs=[cipher suite for IKE]; ike-key=[IKE pre-shared key];</code></td><td>Enters values for additional security parameters for this mgw-profile.
Note This step is optional. Use this command only if you need to modify these values in your system.
Tip The default values of these security parameters are sufficient for some networks. Before making any changes, you can use the <b>show</b> command to determine if changes are needed to any of the default values.</td></tr>
</table>

Provisioning Security Interfaces to the RKS

This section explains how to provision security interfaces to the RKS.

SUMMARY STEPS

1. Add a security policy for the RKS—**add ipsec-policy**.
2. Enables IPsec for the primary and secondary RKS units—**change radius-profile**.
3. Enter values for additional security parameters for this RKS—**change radius-profile** (optional).

Note The token values shown in this section are examples.

DETAILED STEPS

	Command Examples	Purpose
Step 1	`add ipsec-policy id=rks01; src-fqdn=cms-ca1.ciscolab.com; dest-fqdn=rks1.ciscolab.com; action=ipsec;`	Adds a security policy for the RKS. **Note** You must specify at least one source (src-fqdn, src-ipaddr, or src-port), and at least one destination (dest-fqdn, dest-ipaddr, or dest-port). **Note** You cannot specify both a SRC-FQDN and a SRC-IPADDR at the same time. You cannot specify both a DEST-FQDN and a DEST-IPADDR at the same time.
Step 2	`change radius-profile id=[primary RKS id | secondary RKS id]; tsap-addr=[ip-address | ip-address:port-number]; ike-key=<IKE preshared security key>;`	Enables IPsec for the primary and secondary RKS units. **Note** After you enter a value for the ike-key parameter, the system encrypts it and stores the encrypted value. A **show radius-profile** command displays the encrypted value only. There is no way to display the value of the ike-key that you originally entered.
Step 3	`change radius-profile id=[primary RKS id | secondary RKS id]; tsap-addr=[ip-address | ip-address:port-number]; ipsec-sa-esp-cs=[cipher suite for ESP]; ipsec-sa-lifetime=[IPsec SA expiration time]; ipsec-sa-grace-period=[expiration grace period]; ipsec-ulp-name=[SA upper layer protocol]; ike-group=[1|2]; ike-sa-lifetime=[IKE SA expiration time]; ike-cs=[cipher suite for IKE];`	Enters values for additional security parameters for this radius-profile. **Note** This step is optional. Use this command only if you need to modify these values in your system. **Tip** The default values of these security parameters are sufficient for some networks. Before making any changes, you can use the **show** command to determine if changes are needed to any of the default values.

Provisioning IPsec Security Associations and Ciphersuite Algorithms

This section explains how to provision the IPsec security associations (SAs) and the ciphersuite encryption and authentication algorithms.

- The IPsec SA (ipsec-sa) table contains the IPsec SAs that are not associated with IKE or Kerberos key management.
- A cipher is an algorithm that transforms data between plain text and encrypted text. A ciphersuite consists of both an encryption algorithm and a message authentication algorithm. The Ciphersuite Profile (ciphersuite-profile) and Ciphersuite (ciphersuite) tables provision the allowed ciphersuites for media security (encryption of bearer-path data) between two MTAs.

SUMMARY STEPS

1. Add a security association for a device—**add ipsec-sa**.
2. Create a ciphersuite profile—**add ciphersuite-profile**.
3. Create the ciphersuite data supporting the ciphersuite profile—**add ciphersuite**.

Note The token values shown in this section are examples. For a complete list of tokens and detailed descriptions, see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

DETAILED STEPS

	Command Examples	Purpose
Step 1	**`add ipsec-sa id=cmts01; auth-algo=HMAC-SHA-1; auth-key=2069732061206b6579206f66203234206368612e; dest=10.10.7.7; encrypt-algo=DES; encrypt-key=4bb586a120532c07; spi=-85723; src=10.10.2.2; soft-lifetime=3600; hard-lifetime=7200;`**	Adds a security association for a device. **Note** The range of values is 1 to 8 ASCII characters. The suggested format is <device-type>NN, for example, mta01, cmts01, rks01. This token is mandatory. **Note** After you enter a value for the auth-key and encrypt-key parameters, the system encrypts them and stores the encrypted values. A **show ipsec-sa** command displays the encrypted values only. There is no way to display the values that you originally entered for these two parameters.
Step 2	**`add ciphersuite-profile id=cp1gold; description=This ID is used for QoS gold.`**	Creates a ciphersuite-profile.

Step 3	**`add ciphersuite id=cp1gold; proto-type=RTP; auth-algo=RTP-MMH-4; encrypt-algo=RTP-3DES-CBC; priority=1;`**
	`add ciphersuite id=cp1gold; proto-type=RTCP; auth-algo=RTCP-HMAC-MD5-96; encrypt-algo=RTCP-AES-CBC; priority=1;`
		Creates the ciphersuite data supporting the ciphersuite-profile.

Provisioning Event Messages

This section explains how to provision EM functionality on the Cisco BTS 10200 Softswitch. It includes the following tasks:

- Provisioning Support for EM Transmission and Storage, page 31
- Provisioning the System to Generate EMs for Billing, page 33
- Provisioning Media_Alive Verification for EMs, page 35

Provisioning Support for EM Transmission and Storage

The commands in the following procedure specify the required IDs for the primary and secondary RKSs and link them with the Call Agent (CMS/MGC). They also control parameters related to the transmission of EMs to the RKS and parameters related to storage of EMs on the CA.

- The RADIUS Profile (radius-profile) table is required in PacketCable networks that use an EM-based billing system and a RADIUS-based Record Keeping Server (RKS). This table includes provisionable parameters such as primary and secondary RKS node IDs, IP address and port address, RADIUS retry intervals and retry counts.
- The call-agent-profile table establishes a link between the Call Agent (CMS) and the primary and secondary RKSs.

SUMMARY STEPS

1. Create the interfaces to the primary and secondary RKSs—**add radius-profile**.
2. Specify parameters for storage of EM files on the CA—**change ca-config**.
3. Provision batch mode handling of EMs—**change ca-config**.
4. Set the DSCP for signaling packets on RADIUS interfaces between the CMS and RKS—**change ca-config**.
5. Set the EM privacy indicator token if you want the system to populate the privacy indicator field in the EMs—**change ca-config**. (Applicable to Release 4.5.1 only.)

DETAILED STEPS

Note The token values shown in this section are examples. These tables have many additional optional tokens not shown in these examples. For a complete list of all the tokens for each table, see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

DETAILED STEPS

	Command Examples	Purpose
Step 1	**add radius-profile id=prirks; tsap-addr=192.168.100.100; encryption-key=abcdef1234567890; acc-rsp-timer=7; acc-req-retransmit=4; description=primary_billing_server** **add radius-profile id=secrks; tsap-addr=192.168.100.101; encryption-key=abcdef1234567890; acc-rsp-timer=6; acc-req-retransmit=2; description=secondary_billing_server**	Creates the interfaces to the primary and secondary RKS units and sets values for various parameters. **Note** The ACC-RSP-TIMER and ACC-REQ-RETRANSMIT tokens control the retransmission of EMs from the CA to the RKSs when the first attempt does not go through. ACC-RSP-TIMER controls how long the system waits before retransmitting, and ACC-REQ-RETRANSMIT controls how many retransmission attempts are made to the target RKS.

Step 2	**change ca-config type=retry-pri-rks-timer; datatype=integer; value=14;**
	change ca-config type=em-file-open-time; datatype=integer; value=900;
	change ca-config type=em-file-size; datatype=integer; value=50;
		Specifies how the system stores EMs in files on the CA (when loss of communication with the RKSs prevents EMs from being transmitted to the RKSs).
		Note An open EM file does not close automatically when communication to the RKS is restored. The file closes automatically according to the provisioned value in EM-FILE-OPEN-TIME or EM-FILE-SIZE, whichever occurs first.
		Tip The command is shown as **change ca-config**. However, if the system responds that the parameter does not exist, reenter the command as **add ca-config**.

Step 3	**change ca-config type=batch-mode-supp; value=Y;**
	change ca-config type=batch-latency; value=240;
		Provisions batch mode handling of EMs.
		Tip The command is shown as **change ca-config**. However, if the system responds that the parameter does not exist, reenter the command as **add ca-config**.

Step 4	**change ca-config type=RADIUS-DSCP-TOS; value=240;**	Sets the DSCP for signaling packets on RADIUS interfaces between the CMS and RKS. **Tip** The command is shown as **change ca-config**. However, if the system responds that the parameter does not exist, reenter the command as **add ca-config**.

	Command Examples	Purpose
Step 5	`change ca-config type=EM-PRIVACY-IND-SUPP; datatype=BOOLEAN; value=Y;`	(Release 4.5.1 only) Instructs the system to include the privacy-indicator field in the signaling start EM. For details of this field, see the "EM Generation Details and Content" section on page 44. **Note** This change takes effect immediately when provisioned. It is not necessary to restart any platforms. **Tip** The command is shown as **change ca-config**. However, if the system responds that the parameter does not exist, reenter the command as **add ca-config**.

Provisioning the System to Generate EMs for Billing

The Cisco BTS 10200 Softswitch can provision billing support using either call detail blocks (CDBs), which are assembled into call detail records (CDRs) by an external billing server, or PacketCable EMs, which are transferred to an external RKS that assembles CDRs from the EMs.

The Cisco BTS 10200 Softswitch contains two PacketCable-based logical network elements, the CMS and MGC. The CMS and MGC have provisionable element IDs as described in this section. The applicable element ID is included in each EM sent from the CMS or MGC.

To provision the Cisco BTS 10200 Softswitch to generate EMs for billing, complete the steps shown in the following section.

SUMMARY STEPS

1. Display the current CA profile—**show call-agent-profile**.
2. Modify CA profile parameters related to EM generation and RKS profiles, if necessary—**change call-agent-profile**.
3. Identify the CMS and MGC logical network elements, and the financial entity ID (FEID)—**change call-agent-profile**.
4. (Optional) Provision a billing type (flat rate or measured rate) and an account ID for individual subscribers—**change subscriber**.

DETAILED STEPS

Note The token values shown in this section are examples. In addition, these tables have many additional optional tokens not shown in these examples. For a complete list of all the tokens for each table, see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

DETAILED STEPS

	Command Examples	Purpose
Step 1	`show call-agent-profile id=CA146;`	Displays the current parameters for the CA profile.

Step 2	`change call-agent-profile id=CA146; cdb-billing-supp=N; em-billing-supp=Y; pri-rks-profile-id=prirks; sec-rks-profile-id=secrks;`
	`add call-agent-profile id=CA146; cdb-billing-supp=N; em-billing-supp=Y; pri-rks-profile-id=prirks88; sec-rks-profile-id=secrks88;`
		If the system response (in the display from Step 1) contains data, use the **change call-agent-profile** command if you want to change any of the parameter values.
		If the system response (in the display from Step 1) indicates that this table does not exist, then you must create it using the **add call-agent-profile** command. Otherwise, the EM function is not supported and EMs are not generated.
		Caution If the call-agent-configuration table is not created, the Cisco BTS 10200 Softswitch generates CDBs but not EMs.
		EM and CDB Billing Options
		In a PacketCable network, the service provider can choose EM-based billing or CDB-based billing.
		Caution We strongly recommend that you *do not* set both of these tokens (EM and CDB billing support) to **y**. Attempting to generate both types of records simultaneously can significantly degrade system performance.
		Note To set both tokens to **y**, you must also include **forced=y** in the command line.
		Note Provisioning changes for cdb-billing-supp and em-billing-supp take effect only after a CA switchover or restart.
		RKS IDs
		The value for pri-rks-profile-id (primary RKS profile ID) must be the same as the value for the radius-profile ID for the primary RKS, and the value for sec-rks-profile-id (secondary RKS profile ID) must be the same as the radius-profile ID for the value for the secondary RKS.

	Command Examples	Purpose
Step 3	**`change call-agent-profile id=CA146; cms-id=12345; mgc-id=67890; feid=feid0001;`**	Identifies the CMS and MGC logical network elements and the financial entity ID (FEID). The system uses these IDs when generating EMs. **Note** The Cisco BTS 10200 Softswitch contains both the CMS and MGC logical entities. For PacketCable systems, the CMS-ID must be entered. If your Cisco BTS 10200 Softswitch communicates with a TGW, you must enter the MGC-ID. The FEID value is also required for EM billing. **Note** You must provision the CMS-ID and MGC-ID tokens so that the Cisco BTS 10200 Softswitch can provide support for the Communication Assistance for Law Enforcement Act (CALEA). For provisioning procedures related to CALEA support, see the *Cisco BTS 10200 Softswitch Provisioning Guide.*
Step 4	**`change subscriber ID=SUB5551212; sub-profile-id=profile777; account-id=123456789; billing-type=FR2;`**	(Optional) Provision a billing type (flat rate or measured rate) and an account ID for individual subscribers.

Provisioning Media_Alive Verification for EMs

Use the Activity (activity) table to schedule and configure Media_Alive EMs. These EMs are used during longer-duration calls to verify that the media connection is still alive. For information on these operational commands, see the "Viewing Media_Alive Verification for EMs" section on page 39.

Note For an additional sample provisioning sequence, see the *Cisco BTS 10200 Softswitch Provisioning Guide*. For additional reference information on CLI tables and parameters, see the *Cisco BTS 10200 Softswitch Command Line Interface Guide*.

Operations, Billing, and EM Transfer Procedures

This section covers the operational features of the Cisco BTS 10200 Softswitch PacketCable implementation, including the following topics:

PacketCable Billing Data and Formats in Deployments Using CDBs

For deployments that use CDBs for billing (rather than EMs), the following CMTS and eMTA identifying information is included in the CDBs:

- Billing field 82, Overall correlation identifier
- Billing field 158, originating end point TSAP address
- Billing field 159, terminating end point TSAP address
- Billing field 160, originating CMTS ID
- Billing field 161, terminating CMTS ID
- Billing field 162, originating fiber node ID
- Billing field 163, terminating fiber node ID

See the Appendix A of the *Cisco BTS 10200 Softswitch Billing Guide* for a complete list of billing fields and field contents, and a description of the options for CDB file-naming conventions.

Status Command

The system supports a status command that displays the operational service state of external interfaces. For example, the **status aggr** command displays the operational service state of the CMTS.

Note For the STATUS AGGR command, the available displayed values include INS (in service), OOS (out of service), and CONNECTING. CONNECTING state means that the Cisco BTS 10200 Softswitch is reattempting to connect to the CMTS.

Manual Recovery and Transfer of Stored EMs

This section describes how to manually recover and transfer stored EM files from the CA to the RKS. This procedure must be used if communication to both RKS units goes down. Perform these procedures after communication is restored.

Recovering the Billing Files

Note For information on compliance with specific paragraphs of PacketCable standards and ECNs, contact your Cisco account team.

Billing data is normally transferred to the RKS on a real-time basis. In the unlikely event that communications with the RKS go down, alarms are raised and billing data files are written to a local drive on the Cisco BTS 10200 Softswitch (see the /opt/BTSem directory on the Call Agent (CA) that generated the EMs). If communications are not promptly restored, additional billing alarms of increasing severity are raised at time intervals of 1 hour (minor), 3 hours (major), and 5 hours (critical).

EMs that are not successfully transferred to the RKS are stored on the Call Agent. The system uses the naming conventions specified in PacketCable ECN EM-N-04.0186-3 for the stored EMs. Here is the format for the file name:

PKT_EM_<yyyymmddhhmmss>_<priority>_<record type>_<node id>_<sequence>.bin

The parameters are defined as follows:

PKT_EM is fixed and does not change across files.

- **yyyymmddhhmmss** is a timestamp, where:
  - **yyyy** is the year, such as 2005
  - **mm** is the month, from 01 through 12
  - **hh** is the hour, from 00 through 23
  - **mm** is the minute, from 00 through 59
  - **ss** is the second, from 00 through 59
- **priority** is always set to 3.
- **record type** is always set to 0.
- **node id** is the CMS ID or MGC ID. It must be five digits long, padded with leading 0s if necessary. (The system uses the CMS ID or the MGC ID depending on whether the file contains EMs generated by the CMS or the MGC function of the Call Agent.)
- **sequence** is the file sequence number. It must be six digits long, padded with leading 0s if necessary. (The CMS and MGC files are numbered independently.)
- **.bin** is the binary file type designation.

Here is an example of a typical EM file name:

PKT_EM_20050915103142_3_0_01234_000002.bin

All billing data generated during the period of the communication outage is stored in the /opt/BTSem directory. If communication with the RKS is lost for an extended period, the available disk space on the local Softswitch drives can begin to fill up with EM files. The system monitors the amount of space available on the disks and raises alarms of increasing severity when the disks are 50 percent (minor), 70 percent (major) and 100 percent (critical) full.

Note There can be billing data files on both CAs, primary and secondary, depending on whether there have been any switchovers during the loss of communication with the RKS.

We recommend that you monitor the available disk space on a regular basis to prevent the possible loss of billing data. If the disks become full, the data on the disk is preserved and new EMs are discarded.

Caution Do not allow the disk to become full. If you do not transfer the billing data files to the RKS, billing data might be lost. If EMs are discarded, they cannot be recovered and revenue could be lost.

Sending Billing Files to the RKS via FTP

To send billing files from the CA to the RKS, perform the following steps:

Step 1 On the CA, navigate to the subdirectory to which the billing data is written.

```
cd /opt/BTSem
```

Step 2 At the prompt, establish an FTP session with the RKS.

```
ftp <RKS name>
```

Step 3 When prompted, enter your user name and password for the RKS. The FTP prompt should appear.

Step 4 At the FTP prompt, enter **bin** to enable binary transfer:

```
bin
```

Step 5 On the RKS, navigate to the subdirectory to which the billing files will be written.

```
cd /.../.../<billing file subdirectory name>
```

Step 6 Place the applicable billing files in the billing files subdirectory.

```
put <billing-filenames>
```

Step 7 After the transfer is complete and the FTP prompt reappears, exit the FTP session.

```
bye
```

Comparing Checksums

To compare the checksums to ensure that the data was transferred correctly, perform the following steps:

Step 1 Log in to the RKS, using your user name and password for that system.

Step 2 Navigate to the subdirectory to which the billing data files were written.

```
cd /.../.../<billing file subdirectory name>
```

Step 3 List the files in the billing directory. The following command lists the files in reverse order by creation date:

```
ls -lrt
```

Step 4 Run a cksum on the files that were backed up.

```
cksum <billing-filename>
```

Step 5 Compare these cksum values to the corresponding cksum values on the CA.

a. If the cksum values are the same, the file transfer has completed without error.

b. If the cksum values are **not** the same, repeat all of the steps in the "Sending Billing Files to the RKS via FTP" section on page 38 and "Comparing Checksums" section on page 38.

If the cksum values are still different, contact Cisco TAC for assistance.

Viewing Media_Alive Verification for EMs

Use the activity table to schedule and configure Media_Alive EMs. These EMs are used during longer-duration calls to verify that the media connection is still alive.

Step 1 Configure Media_Alive generation according to local requirements (example shown here):

```
add activity id=MEDIA-ALIVE-EM; freq=6H; start-time=HH:MM;
```

where:

- **id**—The value must be MEDIA-ALIVE-EM, which is a fixed system value listed in the Activity Base (activity-base) table.

Note You can view other tokens in the activity-base table by using the command **show activity-base**. However, you cannot change any values in that table.

- **freq**—Frequency. The number of times to schedule the specified EM Media_Alive activity.
- **start-time**—Time of day in the format HH:MM ranging from 00:00 to 23:59 (default is 00:00).

Note The activity table has several other tokens that support other EM Media_Alive options. For more detailed information about these options, see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

Step 2 To view the MEDIA-ALIVE-EM activity, enter the following command:

```
show activity id=MEDIA-ALIVE-EM;
```

Sample command line output:

```
ID=MEDIA-ALIVE-EM
FREQ=30 MINUTES
DAY_OF_MONTH=NA
DAY_OF_WEEK=NA
```

```
START_TIME=00:00
FIXED_TIME_INTERVAL=N
ENABLED=N
SO_ENABLED=N
RESTART_ENABLED=N
LAST_CHANGED=2004-10-20 16:45:30
```

Measurements

Several traffic measurements pertain to the PacketCable implementation. For detailed descriptions see the Traffic Measurements section in the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

Creating Reports and Displays of Measurements

This section outlines the procedure for creating reports and displays of measurements. It uses the DQoS feature as an example.

Note Additional details about measurement provisioning, reporting, and display commands for all features can be found in the *Cisco BTS 10200 Softswitch Operations Guide* and the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

To create a report file of the DQoS counters for all time intervals in the period starting and ending at specific times, enter the following command. The system prepends the file with the string "Tm_" and writes the file to the /opt/ems/report directory on the active EMS.

```
report measurement-dqos-summary; start-time=[start-time]; end-time=[end-time];
aggr-id=[ID of the aggregation router (CMTS) for which data should be reported];
output=[desired file name for the report]; output-type=[CSV | XML];
```

where:

start-time and **end-time** have the format yyyy-mm-dd hh:mm:ss

CSV = comma-separated value

Note Time intervals can be every 5, 15, 30, or 60 minutes. This is provisionable in another command, **change measurement-prov**, as described later in this section.

Use any of the following commands to display DQoS counters on your monitor.

- To display DQoS counters for all time intervals in the past 48 hours for all CMTS IDs, enter the following command:

  ```
  report measurement-dqos-summary; interval=ALL;
  ```

- To display DQoS counters tracked at every interval in the period starting at a specific start-time and for all aggregation IDs, enter the following command:

  ```
  report measurement-dqos-summary; start-time=[start-time];

  (start-time has a format of yyyy-mm-dd hh:mm:ss, and the end-time defaults
  to the most recent interval)
  ```

- To display DQoS counters for the most recent time interval for all aggregation IDs, enter the following command:

  ```
  report measurement-dqos-summary;

  (start-time and end-time both default to the most recent interval)
  ```

In this example, the system displays the most recent time interval for all aggregation IDs:

```
report measurement-dqos-summary
Reply: Request was successful.
TIMESTAMP       20020310184428
DQOS_GATESET_ATTMP       10
DQOS_GATESET_SUCC         9
DQOS_GATE_COMMIT          9
```

In this example, the display token is used to specify desired counters (separated by commas):

```
report measurement-dqos-summary;
display=DQOS_GATESET_ATTMP,DQOS_GATE_COMMIT;
Reply: Request was successful.
TIMESTAMP       20020310184428
DQOS_GATESET_ATTMP       10
DQOS_GATE_COMMIT          9
```

To manage the collection of DQoS measurements, use the following commands:

- To display the current provisioning settings of DQoS measurements (enabled or disabled status), enter the following command:

  ```
  show measurement-prov type=DQOS;
  ```

- To change the current provisioning settings of DQoS measurements (enabled or disabled status) and/or the time interval (5, 15 [default], 30, or 60 minutes), enter the following command:

  ```
  change measurement-prov type=dqos; enable=yes; time-interval=30;
  ```

Measurements for the DQoS Feature on COPS Interface

The following DQoS measurements are provided to support the COPS interface.

Tip The Cisco BTS 10200 Softswitch tracks and reports measurements separately for each of the CMTS units (aggregation routers) it supports.

- DQOS_GATESET_ATTMP—The number of DQOS GATE-SET attempts of all types on the reporting CMTS
- DQOS_GATESET_SUCC—The number of successful DQOS GATE-SET attempts of all types on the reporting CMTS

- DQOS_GATE_COMMIT—The number of successfully committed DQOS gates of all types on the reporting CMTS

Measurements for the EM Feature

The following operational measurement counts and/or statistics are supplied for the EM feature:

- BILLING_EM_ACKED—The number of EMs acknowledged by the RKS.
- BILLING_EM_LOGGED—The number of EMs written to disk but not sent to any RKS.
- BILLING_EM_RETRANS—The number of EMs that were transmitted to an alternate RKS due to the lack of a response from a previously tried RKS, excluding retries. The counter is incremented when an EM is first sent to an alternate RKS. Any retries that occur at the RADIUS stack level (as provisioned in the radius-profile table) are not included in this count.

Use the following CLI command to retrieve these measurements:

```
report measurement-em-summary
```

A typical command and system response are shown below:

```
report measurement-em-summary

TIMESTAMP               2003-07-10 16:15:00
CALL_AGENT_ID           CA146
CONDITION               Normal
BILLING_EM_ACKED        2
BILLING_EM_LOGGED       3
BILLING_EM_RETRANS      3
```

Events and Alarms

This section lists the events and alarms applicable to the PacketCable implementation, including:

- Events and Alarms Specific to PacketCable-Based Network Elements, page 42
- Events and Alarms for the EM Feature, page 43
- Events and Alarms for the Security Interface Feature, page 43

Note This section lists only the events and alarms that are specific to the PacketCable-based implementation, and includes only the name and description of each alarm. Detailed descriptions of all events and alarms, and recommended corrective actions, are presented in the *Cisco BTS 10200 Softswitch Operations, Maintenance, and Troubleshooting Guide*.

Events and Alarms Specific to PacketCable-Based Network Elements

The following events and alarms can be generated in response to processing problems or network connection issues with PacketCable-based network elements:

- CALL PROCESSING Event #15—CMTS ER ID Not found in MGW table (INFO)
- SIGNALING Alarm #103—AGGR Connection Down (MAJOR)
- SIGNALING Event #104—AGGR Unable To Establish Connection (INFO)

- SIGNALING Event #105—AGGR GATE-SET Failed (INFO)
- SIGNALING Alarm #106—ESA BTS DF Connection Down (MINOR)

Events and Alarms for the EM Feature

The following events and alarms can be generated by the EM feature.

- BILLING Alarm #38—EM log file access error (MAJOR)
- BILLING Alarm #39—RADIUS accounting receive failure (MINOR)
- BILLING Alarm #40—EM encode failure (MINOR)
- BILLING Alarm #41—Message content error (MINOR)
- BILLING Event #42—Error reading provisioned data—using default (WARNING)
- BILLING Event #44—RKS switch occurred (MAJOR)
- BILLING Event #45—Event Message log file opened (MINOR)
- BILLING Event #46—Event Message log file closed (MINOR)
- BILLING Alarm #47—RKS unreachable for 1 hr (MINOR)
- BILLING Alarm #48—RKS unreachable for 3 hours (MAJOR)
- BILLING Alarm #49—RKS unreachable for 5 hours (CRITICAL)
- BILLING Alarm #53—Event Message disk space 50 percent full (MINOR)
- BILLING Alarm #54—Event Message disk space 70 percent full (MAJOR)
- BILLING Alarm #55—Event Message disk space 100 percent full (CRITICAL)

Events and Alarms for the Security Interface Feature

The following events and alarms can be generated in response to PacketCable-related security signaling conditions:

- SECURITY Alarm #3—IPsec connection down (MAJOR)
- SECURITY Event #4—IPsec MTA Key Establish Error (WARNING)
- SECURITY Event #5—IPsec outgoing SA not found (WARNING)

Announcements

Note The Cisco BTS 10200 Softswitch supports a full range of announcements. However, there are no announcements specific to the PacketCable protocol implementation. For details on the announcement files and announcement provisioning, see the Announcement Server Provisioning and Cause Code to Announcement ID Mapping sections in the *Cisco BTS 10200 Softswitch Provisioning Guide*.

EM Generation Details and Content

This section describes the internal processes for EM generation and the content of the EMs. These processes are based on the *PacketCable Event Message Specification* PKT-SP-EM-I10-040721.

Note The system complies with the RKS EM billing interface requirements of PKT-SP-EM-I10-040721. For information on compliance with specific paragraphs of PacketCable standards, contact your Cisco account team.

Note In Release 4.5.1, a privacy indicator is added to the signaling start EM as shown in this section. This attribute uses the previously undefined field #12 in PKT-SP-EM-I10-040721. This field is populated only if the EM-PRIVACY-IND-SUPP token in the CA-CONFIG table is set to Y, the presentation status (PS) of the incoming call is available, and the Calling Party Number field is also populated in the EM.

EM Generation Details

Table 1 lists the EMs generated by specific call configurations.

Table 1 EMs Generated by Call Configuration

Cisco BTS 10200 Softswitch Generates EMs for ...	Call Configuration		
	On-net to on-net	On-net to off-net	Off-net to on-net
Originating CMS	X	X	
Terminating CMS	X		X
Originating MGC			X
Terminating MGC		X	

Table 2 lists the specific EMs that can be generated by the CMS and MGC.

Table 2 EMs Generated by Logical Entity

Event Message	CMS	MGC
Signaling_Start	X	X
Signaling_Stop	X	X
Interconnect_Start		X
Interconnect_Stop		X
Call_Answer	X	X
Call_Disconnect	X	X
Database_Query	X	
Service_Instance	X	
Service_Activation	X	
Service_Deactivation	X	

Table 2 EMs Generated by Logical Entity (continued)

Event Message	CMS	MGC
Media_Alive	X	X
Time_Change	X	X

Table 3 lists the EMs for a call and the triggers that generate them (single zone scenario only) in the appropriate logical entities running in the Cisco BTS 10200 Softswitch (CMS/MGC).

Table 3 EM Triggers by Logical Entity

Event Message	Originating CMS	Terminating CMS	Originating MGC	Terminating MGC
Signaling_Start	Timestamp: Receipt of NCS NTFY Send: after translation	Prop trigger	1. Receipt of IAM or 2. Receipt of TGCP NTFY	Receipt of Invite (prop)
Signaling_Stop	If T-CMS releases first: receipt of 250RSP to DLCX If O-CMS releases first: before deallocating call block	If O-CMS releases first: receipt of 250RSP to DLCX If T-CMS releases first: before deallocating call block	If T-MGC releases first: upon last of following events: 1. Receipt/transmit RLC from/to SG 2. Receipt/transmit of Ack for TGCP DLCX 3. Receipt/transmit last msg from/to T-CMS (prop) If O-MGC releases first: before deallocating call block	Receipt of 250OK to DLCX
Interconnect_Start			Transmit/receipt of ACM	Transmit/receipt of ACM
Interconnect_Stop			Release of PSTN bandwidth	Release of PSTN bandwidth
Call_Answer	Receipt of 200OK to Invite with call answer	Receipt of NCS NTFY for off-hook of T-MTA	1. Receipt of ANM or 2. Answer ind on op.service	1. Receipt of ANM or 2. Answer ind on op.service
Call_Disconnect	Transmit DLCX or delete connection on errors	Transmit DLCX	1. Receipt of REL or 2. Transmit BYE for REL	1. Receipt of REL or 2. Disconnect ind on op. service trunk disconnect
Database_Query	Receipt of response from DB/Intelligent peripheral	Receipt of response from DB/Intelligent peripheral	—	—
Service_Instance	Operation of service	Operation of service	—	—
Service_Activation	Successful activation	Successful activation	—	—
Service_Deactivation	Successful deactivation	Successful deactivation	—	—

Table 3 EM Triggers by Logical Entity (continued)

Event Message	Originating CMS	Terminating CMS	Originating MGC	Terminating MGC
Media_Alive	Periodic, based on provisioned parameters	Periodic, based on provisioned parameters	Periodic, based on provisioned parameters	Periodic, based on provisioned parameters
Time_Change	When time is adjusted	When time is adjusted	When time is adjusted	When time is adjusted

Table 4 lists the PacketCable 1.0 features, the EMs generated for them, and the event that triggers the message. Some of the triggering events include the logical entities—Originating CMS (O-CMS) and Terminating CMS (T-CMS)—running in the Cisco BTS 10200 Softswitch.

Table 4 PacketCable 1.0 Features and Associated EMs

	EMs Sent in Addition to Basic Call EMs		
PacketCable 1.0 Feature	**Event Message**	**Trigger**	**Comments**
911 service—Similar to on-net to off-net call on a unique trunk group ID.	None	—	—
Other N11 services—Similar to above	None	—	—
Database query			
a. Send all database queries to PSTN on special trunk	None	—	—
b. Query database and route accordingly	db_query	O-CMS on receipt of response to database dip	Query types: 1 = Toll Free Number Lookup 2 = LNP Number Lookup 3 = Calling Name Delivery Lookup If the query is successful—that is, if the query returns the calling party's name—the query type (1, 2, or 3) is included in the EM: • For types 1 and 2, the value in the EM Return_Number field contains the new called party digits. • For type 3, the value in the EM Return_Number field contains a valid string, such as "O" or "P". [1] If the query fails, no EM is sent.
Operator service			
a. 0– service (no digit after 0)	None	Called party number 0 is replaced by Operator Service Provider number.	Only call routing.

Table 4 PacketCable 1.0 Features and Associated EMs (continued)

	EMs Sent in Addition to Basic Call EMs		
PacketCable 1.0 Feature	**Event Message**	**Trigger**	**Comments**
b. 0+ service (digits after 0, not needed in PacketCable 1.0)			Only call routing.
Call block service (with new call to announcement server)	Service instance	O-CMS and T-CMS decide to block call.	If announcement server is connected, event messages are generated for call with same BCID.
Call waiting			
a. Announcement server on net	Service instance	O-CMS and T-CMS when call waiting is initiated. Second call BCID for service instance	Only two calls, one active and one on hold, are required. Each half-call generates an EM. A half-call for an on-net announcement server for call waiting tone need not generate an EM. Here is an example of a call scenario: A calls B, C calls A: (A –> B, C –> A) BCID1 for A(O), other leg BCID2 BCID2 for B(T), other leg BCID1 BCID3 for C(O), other leg BCID4 BCID4 for A(T), other leg BCID3 BCID4 for CW service instance, related BCID = BCID1
b. Announcement server on PSTN	not supported	—	—
Call forwarding	Service instance	CMS (O/T) when forwarded call leg is initiated.	A calls B, B forwards to C: (A –> B –> C) BCID1 for A(O), other leg BCID2 BCID2 for B(T), other leg BCID1 BCID3 for B(O), other leg BCID4 BCID4 for C(T), other leg BCID3 BCID3 for CFW service instance, related BCID=BCID2
Return call (with caller ID privacy restriction)			CMS-CMS signaling is not supported in this release.
a. Announcement server on net	Service instance	O-CMS on feature initiation.	—
b. Announcement server on PSTN	Not supported	—	—
Repeat call (*66)			CMS-CMS signaling is not supported in this release.
a. Announcement server on net	Service instance	Repeat call is initiated.	Separate BCID for service instance.
b. Announcement server on PSTN	Not supported	—	—
Voice mail (voice mail server on off-net)	None	—	—
Deposit and retrieval: similar to on-net to off-net call	None	—	—

Table 4 PacketCable 1.0 Features and Associated EMs (continued)

	EMs Sent in Addition to Basic Call EMs		
PacketCable 1.0 Feature	**Event Message**	**Trigger**	**Comments**
Message waiting indicator	None	—	No event messages for message waiting.
Privacy indicator (Release 4.5.1 only)	Signaling start	—	Indicates whether the system populates field #12 of the EM with the calling party service (privacy setting) for the calling party. This attribute uses the previously undefined field #12 in PKT-SP-EM-I10-040721. See the "EM Content" section on page 49 for additional requirements.

[1] "O" = Name is out of area, unknown, or not available. "P" = Name presentation is restricted.

EM Content

The following EMs for a call contain the attributes listed, and are based on the four logical entities running in the Cisco BTS 10200 Softswitch: Originating CMS (O-CMS), Terminating CMS (T-CMS), Originating MGC (O-MGC), and Terminating MGC (T-MGC).

Signaling Start

Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
Direction Indicator	X	X	X	X
MTA endpoint name	Originating	Terminating	Name of endpoint (EP) in MGW	Name of endpoint (EP) in MGW
Calling party number	X	X	X	X
Calling party service [1] (Release 4.5.1 only)	X	X	X	X
Called party number	X	X	X	X
Routing number	X	X	X	X
Location routing number (LRN)	X	X	X	X
Carrier identification code (CIC)			X	X
Trunk group ID			X	X
Jurisdiction information parameter (JIP)	X	X	X	
Ported-in calling number	X			
Ported-in called number		X		
Calling party NP source	X			
Called party NP source		X		
Billing type (measured rate or flat rate)	X			

[1] The calling party service attribute uses the previously undefined field #12 (see PKT-SP-EM-I10-040721). It is an unsigned integer, four bytes in length. If (a) the EM-PRIVACY-IND-SUPP token in the CA-CONFIG table is set to Y, and (b) the calling party number field in the EM is populated, then the system populates the calling party service field as follows: If the presentation status (PS) of the calling party is set to private, the calling party service field is set to 1; if the PS is set to public, the calling party service field is set to 0. If the EM-PRIVACY-IND-SUPP token is set to N (default), or if the calling party number is not present in the Signaling Start EM, or the PS is not present in the incoming message, the system does not populate the calling party service field.

Signaling Stop

Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
BCID of T-CMS or T-MGC	X		X	
BCID of O-CMS or O-MGC		X		X
FEID of T-CMS or T-MGC	X		X	
FEID of O-CMS or O-MGC		X		X

Interconnect Start

Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
Routing number			X	X
CIC			X	X
Trunk group ID			X	X

Interconnect Stop

Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
CIC			X	X
Trunk group ID			X	X

Call Answer

Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
Charge number	X	X	X	X
BCID of T-CMS or T-MGC	X		X	
FEID of T-CMS or T-MGC	X		X	
BCID of O-CMS or O-MGC		X		X
FEID of O-CMS or O-MGC		X		X

Call Disconnect

Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
Call termination cause	X	X	X	X

Service Instance

Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
Service name (plus specified attributes in the table below)	X	X		
Account code	X			
Authorization code	X			

Note Only a limited number of service names are specified in the PacketCable 1.0 specification. The Cisco BTS 10200 Softswitch supports many other features; however, it does not send EMs for those features to a standard Record Keeping Server (RKS) because the feature codes for those features have not yet been defined by PacketCable.

Service-Specific Attributes	Attribute	Call Forward	Call Waiting	Repeat Call	Return Call	Call Block	Three-Way Call	Privacy Indicator
	Related BCID	X	X				X	
	Charge number	X	X	X	X		X	
	1st call calling party number		X					
	2nd call calling party number		X					
	Called party number		X					
	Routing number			X	X			
	Calling party number			X	X			X
	Calling party service (Release 4.5.1 only)			X	X			X
	Termination cause					X		

Service Activation	Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
	Service name (plus specified attributes in the table below)	X	X		

Service-Specific Attributes	Attribute	Call Forward	Call Waiting	Call Block	Customer Originated Trace
	Charge number	X	X	X	X
	Calling party number	X	X	X	X
	Forwarded number	X			

Service Deactivation	Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
	Service name (plus specified attributes in the table below)	X	X		

Service-Specific Attributes	Attribute	Call Forward	Call Waiting	Call Block
	Charge number	X	X	X
	Calling party number	X	X	X

Database Query

Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
Database ID	X	X		
Query type	X	X		
Called party number	X	X		
Returned number	X	X		

Activity

Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
Media alive	X	X	X	X

Time Change

Attribute	O-CMS	T-CMS	O-MGC (off-net to on-net call)	T-MGC (on-net to off-net call)
Time adjustment	X	X	X	X

References

Related Documents

Related Topic	Document Title
Overview of current release	*Cisco BTS 10200 Softswitch Release Notes*
Technical description	*Cisco BTS 10200 Softswitch System Description*
Provisioning procedures	*Cisco BTS 10200 Softswitch Provisioning Guide*
Provisioning commands reference	*Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*

Industry Standards

Standards	Title
IETF RFC 2748	*The COPS (Common Open Policy Service) Protocol*, January 2000
PKT-SP-CODEC-I04-021018	*PacketCable Audio/Video Codecs Specification*, October 18, 2002
PKT-SP-DQOS-I07-030815	*PacketCable Dynamic Quality of Service Specification*, August 15, 2003
PKT-SP-MGCP-I08-030728	*PacketCable Network-Based Call Signaling Protocol Specification*, July 28, 2003
PKT-SP-TGCP-I05-030728	*PacketCable PSTN Gateway Call Signaling Protocol Specification*, July 28, 2003
PKT-SP-EM-I10-040721 **Note** Compliant with the RKS EM billing interface requirements of PKT-SP-EM-I10-040721.	*PacketCable Event Message Specification*, July 21, 2004
EM-N-04.0186-3 **Note** Compliant with the file-naming convention in EM-N-04.0186-3.	*CableLabs Engineering Change (EC) Form*
PKT-SP-SEC-I09-030728	*PacketCable Security Specification*, July 28, 2003
PKT-SP-ESP-I01-991229	*PacketCable Electronic Surveillance Specification*, December 29, 1999

Note For information on compliance with specific paragraphs of PacketCable standards and ECNs, contact your Cisco account team.