Network and Subscriber Feature Descriptions

Chapter 2 - Lawful Intercept and CALEA

Network and Subscriber Feature Descriptions
Preface
Chapter 1 - Network Features
Chapter 2 - Lawful Intercept and CALEA
Chapter 3 - Subscriber Features
Chapter 4 - COS and OCB Features
Chapter 5 - Feature Interactions
Chapter 6 - IVR Features

Table Of Contents

Download this chapter
Chapter 2 - Lawful Intercept and CALEA
Download the complete book
Network and Subscriber Feature Descriptions - Book Length PDF
(PDF - 4 MB)

GIVE US FEEDBACK

Lawful Intercept and Enhanced CALEA Features

Revised: July 2, 2009, OL-12606-20

This chapter describes the lawful intercept interface supported by the Cisco BTS 10200 Softswitch, along with enhanced CALEA features that were introduced with Release 5.0.

General Description of Lawful Intercept Implementation

The Cisco BTS 10200 Softswitch supports the call data interface and call content function for lawful intercept, along with the provisioning interface required to configure a wiretap. The BTS 10200 provides support for lawful intercept using two different, industry-developed architectures: PacketCable and the Cisco Service Independent Intercept (SII). Depending on their network type, service providers may choose to configure their networks consistent with either of these architectures in their effort to meet their obligations related to lawful intercept. Given the constantly evolving nature of industry-developed standards, service providers must recognize that the features and functionality of the BTS 10200 described below may also be subject to change over time.

Each country controls its own laws applicable to lawful intercept. For example, in the United States, one of the applicable laws is referred to as the Communications Assistance for Law Enforcement Act (CALEA).

Lawful Intercept Provisioning Interface

The BTS 10200 supports a secure provisioning interface to process wiretap requests from law enforcement agencies through a mediation device. The service provider can limit viewing and provisioning of these parameters to selected authorized personnel. The applicable parameters (entered via CLI) include the DN, tap type, and call data channel for data transmission. The tap type specifies whether the tap order is a pen register (outgoing call information), a trap and trace (incoming call information), a pen and trace (incoming and outgoing call information), or an intercept (bidirectional plus the call content).

Note To provision this feature, see the CALEA provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Lawful Intercept Call Data Interface

The BTS 10200 provides the PacketCable EMS/RADIUS interface for the transmission of call identifying information to the lawful intercept delivery function (DF) server as required by Appendix A, PCES Support, in PKT-SP-EM1.5-I02-050812, *PacketCable Event Messages Specification (EMS),* August 12, 2005.

Full call-identifying information (call data) is shipped to a DF server from the BTS 10200 for the subject under surveillance for various call types (for example, basic call and call forwarding).

Lawful Intercept Call Content Function

The call content function provides for capturing voice in a replicated Real-Time Transport Protocol (RTP) stream. The BTS 10200 can be configured to operate with simultaneous support for PacketCable intercept and Cisco SII, or with Cisco SII only.

Simultaneous support for PacketCable intercept and Cisco SII is achieved as follows: During the call-setup phase, the BTS 10200 searches for a PacketCable-compliant call-content intercept access point (IAP) in the call path. If the BTS 10200 determines that there is no such IAP available in the call path, it falls back to Cisco SII.

Note An intercept access point (IAP) is a point within a communication system where some of the communications or call identifying information of an intercept subject's equipment, facilities, and services are accessed.

Additional information about each type of intercept is provided below:

- PacketCable intercept—In PacketCable intercept, a replicated

RTP stream is sent to the DF server by an aggregation router or a trunking gateway upon request from the BTS 10200. The BTS 10200 requests the relevant IAP (aggregation router or trunking gateway) to duplicate and transport the RTP stream to a predefined IP address and port number.

The BTS 10200 uses Common Open Policy Service (COPS) protocol when sending the above request to an aggregation router, and Media Gateway Control Protocol (MGCP) when sending the request to a trunking gateway.

- Cisco Service Independent Intercept—In Cisco SII, a replicated RTP stream is sent to the DF server by an aggregation router or a trunking gateway upon request from the DF server. The DF server uses SNMPv3 as the control protocol to send the intercept request to the appropriate IAP.

Enhanced CALEA Features

This document describes enhancements to the Communications Assistance for Law Enforcement Act (CALEA) feature for the BTS 10200 Release 5.0 and contains the following sections:

- CALEA Enhancement Overview
- Generic CALEA Enhancements
- Surveillance for Calls Involving Multiple CMSs
- BTS 10200 CALEA Interaction with SIP Endpoints
- Changes to Interface between the BTS 10200 and Delivery Function Server
- BTS 10200 CALEA Interaction with SIP Triggers Feature
- CALEA Backward Compatibility
- Compliance with CALEA Requirements in PKT-SP-EM1.5-I01-050128 Appendix A
- Compliance with CALEA Requirements in PKT-SP-CMSS1.5-I01-050128 Section 7.7.2

CALEA Enhancement Overview

CALEA features were enhanced in Release 5.0 to comply with the PacketCable specifications. In addition to generic CALEA enhancements as specified in PacketCable specifications, this section includes clarifications for surveillance functions performed by the Cisco BTS 10200 when the subscriber under surveillance is configured as a SIP endpoint and when the call under surveillance involves multiple CMSs.

The CALEA feature enhancements comply with the following PacketCable specifications:

- PacketCable 1.5 Event Message Specification, PKT-SP-EM1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc. (Appendix A: EM CALEA Requirement Compliance)
- PacketCable 1.5 Call Management Server Specification, PKT-SP-CMSS1.5- I01-050128, January 28, 2005, Cable Television Laboratories, Inc. (Section 7.2.2: CMSS CALEA Requirement Compliance)

Generic CALEA Enhancements

When an origination or termination attempt is detected for a call under surveillance, the BTS 10200 issues call-data event messages to the Delivery Function device to provide call-identifying information. The BTS 10200 follows the procedural and encoding guidelines specified in PKT-SP-EM1.5-I01-050128 Appendix A for sending these event messages. Table 2-1 lists all the call-data event messages supported by the BTS 10200.

Table 2-1 CALEA Call-Data Event Messages Supported by the BTS 10200

Message	Description
Signaling Start	The BTS 10200 generates this message whenever an origination attempt or termination attempt is detected for a call under surveillance.
Media Report	The BTS 10200 generates this message when SDP information from both sides of the call is available for the call under surveillance.
Call Answer	The BTS 10200 generates this message whenever a call under surveillance moves to the answered state.
Call Disconnect	The BTS 10200 generates this message whenever a call under surveillance moves to the disconnected state.
Signaling Stop	The BTS 10200 generates this message when a call under surveillance has ended.
Service Instance	The BTS 10200 generates this message when a feature is invoked by the BTS 10200 for the subject under surveillance. **Note** The BTS 10200 does not send this message if it is not aware of a service invocation (for example, a Call Waiting at a SIP endpoint).
Signal Instance	The BTS 10200 generates this message whenever it receives information from the subject or sends information to the subject. **Note** The BTS 10200 cannot (and is not required to) report some signals if the tapped user has a SIP endpoint (refer to Table 2-3 for detailed information) or for cases in which the BTS10200 does not apply the signal itself to NCS endpoints. For example, the Ringback signal is not applied and not reported to the DF if the media-gateway of the terminating party (C) is able to provide the remote ringback. **Note** This message is new in

Redirection	The BTS 10200 generates this message if call forwarding/transfer is invoked by the BTS 10200 for the associate of the subscriber under surveillance. **Note** This message is new in Release 5.0.
Surveillance Stop	The BTS 10200 generates this message when the surveillance function for a call under surveillance ends. **Note** This message is new in Release 5.0.
Conference Party Change	The BTS 10200 generates this message if the subscriber under surveillance joins two calls (using the Three-way call feature on BTS) and if one of the communicating parties subsequently leaves the conference. **Note** The BTS 10200 does not send this message if it is not aware of the three-way call (for example, a three-way call at a SIP endpoint). **Note** This message is new in Release 5.0.

Detailed information about compliance with the requirements in specification PKT-SP-EM1.5- I01-050128 Appendix A is provided in Table 2-4.

Surveillance for Calls Involving Multiple CMSs

When a call under surveillance spans multiple call management systems (CMSs), one CMS might not have access to all call identifying information or call-content intercept-access points to perform surveillance. RFC-3603 and PKT-SP-CMSS1.5-I01-050128 specify the procedure for a CMS to request other adjacent CMSs to perform surveillance on its behalf. According to these procedures, a CMS can request a CMST (CMS at the terminating side of the call) or a CMST (CMS at the originating side of the call) to perform surveillance functions. The CMS uses the SIP P-DCS-LAES header to make the request.

The Cisco BTS 10200 supports the sending and receiving of the P-DCS-LAES header in various SIP messages using guidelines specified in PacketCable specification PKT-SP-CMSS1.5-I01-050128. The detailed compliance with the procedures specified in the PKT-SP-CMSS1.5- I01-050128 specification is provided in Table 3. The following statements describe how the Cisco BTS 10200 uses the SIP P-DCS-LAES header to implement CALEA.

- When the BTS 10200 requires assistance from another CMS to perform the call-data surveillance function or call-data and call-content surveillance function, it includes the SIP

P-DCS-LAES header in a SIP message. Depending on the call scenario, the following SIP messages can carry the P-DCS-LAES header as an indication of a surveillance request sent to the CMST or CMS:

  - INVITE (or RE-INVITE) message
  - 183 Progress
  - 180 Alerting
  - 200 OK
  - 302 Redirection

- When the BTS 10200 requires the assistance of an adjacent CMS in performing the call-data surveillance function, it includes BCID, CDC-IP-Address, and CDC-IP-Port information in the SIP P-DCS-LAES header.
- When the BTS 10200 requires the assistance of an adjacent CMS to perform the call-data and call-content surveillance functions, it includes BCID, CDC-IP-Address, CDC-IP-Port, CCC-ID, CCC-IP-Address, and CCC-IP-Port information in the SIP P-DCS-LAES header.
- When the BTS 10200 receives P-DCS-LAES header information in any of the following SIP messages, it takes on the surveillance responsibility based on the content of SIP P-DCS-LAES header.
  - The BTS 10200 assumes the responsibility of Call-Data surveillance if the P-DCS-LAES header is included in a SIP message with valid BCID, CDC-IP-Address, and CDC-IP-Port information.
  - The BTS 10200 assumes the responsibility of Call-Data and Call-Content if the P-DCS-LAES header is included in a SIP message with BCID, CDC-IP-Address, CDC-IP-Port, CCC-ID, CCC-IP-Address, and CCC-IP-Port information.

  The grammar for the P-DCS-LAES header is specified in two documents: PKT-SP-CMSS1.5-I01-050128 Section 7.7.2.1 and RFC 3603 Section 8. The BTS 10200 conforms to the grammar rules specified in PKT-SP-CMSS1.5-I01-050128 Section 7.7.2.1 for the encoding and decoding of the P-DCS-LAES header.

P-DCS-Redirect	= "P-DCS-Redirect" HCOLON Called-ID *(SEMI redir-params)
Called-ID	= LDQUOT addr-spec RDQUOT
redir-params	= redir-uri-param / redir-count-param /generic-param
redir-uri-param	= "redirector-uri" EQUAL Redirector
Redirector	= LDQUOT addr-spec RDQUOT
redir-count-param	= "count" EQUAL Redir-count
Redir-count	= 1*DIGIT

BTS 10200 CALEA Interaction with SIP Endpoints

The BTS 10200 Softswitch follows the guidelines specified in PKT-SP-EM1.5- I01-050128 Appendix A for sending call-identifying information to the delivery function for SIP endpoints. While attempting to deliver call-content information, the BTS 10200 notifies the DF server about the unavailability of call-content IAP on either the originating side or terminating side of the call. These packet-cable compliant call-content IAPs typically are not available when the caller and called are SIP endpoints. In order to capture call-content information for these cases, the Delivery Function Server must use the Service Independent Intercept (SII) architecture and initiate a request for duplication of RTP streams.

Note the following additional clarifications about satisfying CALEA requirements for SIP endpoints:

- If feature functionality is provided at the endpoint, the BTS 10200 does not receive any explicit indication about the feature provided by the endpoint. Therefore the BTS 10200 is not required to send Service Instance messages indicating invocation of a feature.
- The requirements in PKT-SP-EM1.5- I01-050128 Appendix A that pertain to sending Signal Instance messages is explicitly designed for NCS/MGCP endpoints. If a tapped subscriber is using SIP endpoints, the BTS 10200 does not instruct the endpoint to play any signals/tones towards the user explicitly. However, the BTS 10200 may send information in SIP messages that trigger an endpoint to play tone or display information to the user. Table 2-2 defines how the BTS10200 behaves with regard to sending Signal Instance messages when a tapped subscriber is using a SIP endpoint.

Table 2-2 Signals Supported for Signaling Instance Messages to SIP Endpoints

Signal Type	BTS 10200 Behavior
Busy Tone	BTS10200 reports SIGNAL INSTANCE message with Audible tone = BUSY when it sends a 486 busy towards the SIP endpoint under surveillance.
Calling Name/Number	BTS10200 reports SIGNAL INSTANCE message with Terminal Display attribute containing Calling Name, Calling Number, and Date if they are included in the INVITE message sent toward the subject with SIP endpoint.
Ringing Tone	BTS10200 reports SIGNAL INSTANCE message with Audible signal = ringing when it receives a 180 Alerting from the subject with SIP endpoint. **Note** In this case, the SIP Endpoint might have played a call-waiting tone instead towards the user.
Distinctive Ringing Tone	BTS10200 reports SIGNAL INSTANCE message with Audible signal = distinctive ringing when it receives a 180 Alerting from the subject with SIP endpoint and the BTS10200 included the Alert-Info header in the SIP INVITE message sent towards the user. **Note** In this case, the SIP Endpoint might have played a call-waiting tone or a normal ringing tone instead towards the user.
Ring back tone	BTS10200 reports SIGNAL INSTANCE message with Audible signal = ringing after sending an 180 Alerting to the subject with SIP endpoint.
Reorder tone	BTS 10200 reports SIGNAL INSTANCE message with Audible signal = reorder-tone when it receives an INVITE message that is processed but cannot be routed due to reasons such as Invalid destination

Table 2-3 specifies the SIGNALS that are not reported by BTS10200 when a tapped user is associated with a SIP endpoint.

Table 2-3 Unsupported Signals for Signaling Instance Messages to SIP Endpoints

Signal Type	BTS 10200 Behavior
Stutter Dial tone	BTS10200 does not request the SIP endpoint to play a Stutter Dial tone.
Confirmation Tone	BTS10200 does not request thee SIP endpoint to play a confirmation tone.
Dial tone	BTS10200 does not request the SIP endpoint to play Dial tone.
Off-hook warning tone	BTS10200 does not request SIP endpoint to play off-hook warning tone. Endpoint may decide to play this tone depending on its own capability or configuration.
Ring Splash	BTS10200 does not request the SIP endpoint to play a Ring splash.
DTMF tones	BTS10200 does not send out-of-band DTMF signals towards SIP endpoints.
Call Waiting tone	BTS10200 cannot detect when a SIP endpoint plays a call-waiting tone towards the user interface. Call Waiting tone is a SIP endpoint feature.

Changes to Interface between the BTS 10200 and Delivery Function Server

This section summarizes how the message interface between the BTS 10200 and the Delivery Function server differs from the preceding BTS 10200 release.

- The BTS 10200 Release 5.0 implements the following additional messages along with the associated attributes to deliver call-identifying information towards the Delivery function server. The details of the message and associated attributes are provided in PKT-SP-EM 1.5-101-050128, Appendix A.
  - Signal Instance
  - Redirection
  - Surveillance Stop
  - Conference Party Change
- The BTS 10200 Release 5.0 also implements the Electronic

Surveillance Indication attribute in the Signaling Start message as defined in PKT-SP-EM 1.5-101-050128, Appendix A. However, this attribute can be used in many call scenarios other than those explicitly presented in packet-cable specifications. The BTS 10200 implements this attribute according to the following guidelines:

  - The BTS 10200 includes the Electronic Surveillance Indication attribute in a Signaling Start message sent from the forwarded-to party in case the call was already under surveillance as a result of a wiretap on the party forwarding the call.
  - The BTS 10200 includes the Electronic Surveillance Indication attribute in a Signaling Start message sent from the final terminating party in case surveillance responsibility is transferred to the BTS from other parties involved in the call due to their inability to perform complete surveillance.
  - The BTS 10200 includes the Electronic Surveillance Indication attribute in a Signaling Start message sent from an originating party in case surveillance responsibility is transferred to the BTS from other parties involved in the call due to their inability to perform complete surveillance.

- The message flows between the BTS 10200 and the Delivery Function server have changed for call-forwarding and call-redirection cases since the preceding release. The changes ensure that a common logic can be used at the Delivery Function server without regard to the number of CMSs and the number of taps involved in the call path. The following case shows the changes to the interface between the BTS 10200 and delivery function server.

Scenario Example

A@cms1 calls B@cms1. B@cms1 has an active call-forwarding unconditional feature to forward all calls to C@cms1. B is the tapped party in this call scenario.

The BTS 10200 Release 4.5 implementation uses the following messages to send call-identifying information to the Delivery Function server:

—> DF (BCID-Bt) Signaling Start (Terminating) (Calling: A) (Called: B)

—> DF (BCID-Bo) Signaling Start (Originating) (Calling: A) (Called: C) (ESI Remote-BCID: (BCID-Bt))

—> DF (BCID-Bo) Service Instance (Call Forward) (Related-BCID: BCID-Bt) (Redirected-From: B) (Redirected-To: C)

—> DF (BCID-Bo) Media Report (Open) (CCCID: X)

—> DF (BCID-Bo) Call Answer (Charge Number: B)

---------------- Active Call under surveillance ------------------------------

—> DF (BCID-Bo) Media Report (Close) (CCCID: X)

—> DF (BCID-Bo) Call Disconnect

—> DF (BCID-Bo) Signaling Stop

—> DF (BCID-Bt) Signaling Stop

The BTS 10200 Release 5.0 implementation uses the following messages to send call-identifying information to the Delivery function server:

—> DF (BCID-Bt) Signaling Start (Terminating) (Calling: A) (Called: B)

—> DF (BCID-Bo) Signaling Start (Originating) (Calling: A) (Called: C) (ESI Remote-BCID: (BCID-Bt))

—> DF (BCID-Bt) Signal Instance (Network Signal) (rs) (Signal-To-Party: B)

—> DF (BCID-Ct) Signaling Start (Terminating) (Calling: A) (Called: C) (ESI Remote-BCID: (BCID-Bo))

—> DF (BCID-Bo) Service Instance (Call Forward) (Related-BCID: BCID-Bt) (Redirected-From: B) (Redirected-To: C)

—> DF (BCID-Ct) Media Report (Open) (CCCID: X)

—> DF (BCID-Ct) Signal Instance (Network Signal) (rg) (Signal-To-Party: C)

—> DF (BCID-Ct) Call Answer (Charge Number: B)

---------------- Active Call under surveillance -----------------------------

—> DF (BCID-Bt) Signaling Stop

—> DF (BCID-Ct) Media Report (Close) (CCCID: X)

—> DF (BCID-Bo) Signaling Stop

—> DF (BCID-Ct) Call Disconnect

—> DF (BCID-Ct) Signaling Stop

—> DF (BCID-Ct) Surveillance Stop (End of Surveillance)

BTS 10200 CALEA Interaction with SIP Triggers Feature

To use the SIP triggers feature functionality (not defined by the PacketCable 1.5 specifications) on the BTS 10200, a call can be routed to an external application server for feature processing. The BTS 10200 supports two types of triggers: Originating Trigger and Terminating Trigger. For both types, when a trigger is detected, the BTS 10200 routes the call to the application server through a SIP interface. Typically, the application server executes the feature logic and performs one of the following two operations to enable the BTS 10200 to route the call to the final destination.

- An application server might initiate a new call (by sending a new INVITE message) to the BTS 10200 and include a SIP header to enable the BTS 10200 to associate the new call with the original call for which feature logic was invoked.
- An application server might send a 3XX redirect back to the BTS 10200 when feature logic processing is complete.

The rest of this section summarizes how the BTS 10200 operates and interacts with the application server to perform surveillance on calls for which the Originating or Terminating Trigger feature is invoked.

When the BTS 10200 detects any origination or termination attempt, it checks for active surveillance associated with the originating or terminating party before routing the call to the application server. If the subscriber is under surveillance, the

BTS 10200 sends a Signaling Start message to the Delivery Function server and performs the call-content surveillance function on an available call-content Intercept access point. In addition, when the call is being routed to the application server, the BTS 10200:

- Initiates a new Signaling Start message with Electronic Surveillance Indication attribute containing the billing-correlation-id set to the billing-correlation-id included in the previous Signaling Start message sent to the Delivery Function server.
- Includes a P-DCS-LAES header with a billing-correlation-id associated with the terminating half of the call.

If the application server redirects the call-back to the BTS 10200, the BTS 10200 forwards the surveillance to the terminating side of the call. However, if the application server initiates a new call (by sending new INVITE message) to the BTS 10200, the BTS 10200 expects the same (unchanged) P-DCS-LAES header (sent earlier on the original call) in the new INVITE message. The BTS 10200 performs the following operations when it receives an INVITE message from the application server:

- Initiates a new Signaling Start message with Electronic Surveillance Indication attribute containing the billing-correlation-id set to the billing-correlation-id included in the previous Signaling Start message sent to the Delivery Function server
- Transfers the surveillance towards the terminating side of the call

In addition, if the surveillance function cannot be performed on the terminating side of the call, the BTS 10200 includes a new P-DCS-LAES header in an 18X or 200 response sent back to the application server. It is assumed that the application server can include the P-DCS-LAES header in a SIP Response message sent back to the BTS 10200 on the original call.

CALEA Backward Compatibility

The Enhanced CALEA feature in Cisco BTS 10200 Release 5.0 implements new messages and attributes defined in newer versions of the PacketCable specifications. In addition, the BTS 10200 has enhanced the internal algorithms to select the call-content IAPs according to the requirements associated with support of the P-DCS-LAES header for performing the surveillance function across multiple CMSs. These enhancements required additional development in the Delivery Function server so that it could continue performing surveillance functions for call-scenarios that include a single CMS or multiple CMSs. For a case in which the event Enhanced Delivery function server is not available, the BTS 10200 provides configuration options (EM-PROTOCOL-VERSION-MAJOR and EM-PROTOCOL-VERSION-MINOR flags in the ESS table) which enable the BTS to interoperate with existing software versions of the Delivery Function server.

Note By using the configuration options, the BTS 10200 provides backward compatibility by disabling the new messages and attributes implemented in BTS10200 Release 5.0. However, BTS 10200 Release 5.0 does not provide backward compatibility to permit selecting the call-content IAP to generate the duplicate call-content based on the algorithm implemented in older releases of the BTS 10200 software.

Note The BTS 10200 enables use of the version flags that provide backward compatibility for certain requirements (or implementations) to avoid interoperation problems with the current version of the Delivery Function server. However, the BTS 10200 does *not* provide control for *all* of the different versions of the PacketCable specifications that describe the use of these flags.

CALEA Operation Similar to BTS Release 4.5

To configure CALEA to operate as it did for BTS 10200 Release 4.5, set the following ESS table tokens as follows:

Option 1

- EM-PROTOCOL-VERSION-MAJOR = 11
- EM-PROTOCOL-VERSION-MINOR = 06
- GENERAL-PURPOSEFLAG = 1

In this configuration, the BTS 10200 does not send the P-DCS-LAES header and ignores the receipt of the P-DCS-LAES header. The BTS also disables support of all the new messages implemented on top of BTS 10200 Release 4.5 (which include, SIGNAL INSTANCE, REDIRECTION, CONFERENCE PARTY CHANGE, SURVEILLANCE STOP). Furthermore, the BTS disables the Electronic Surveillance Indication attribute in the Signaling Start message. In addition, the BTS 10200 does not attempt to forward the surveillance responsibility towards the terminating party in call-forwarding situations, assuming that the forwarding party remains in the call path for the duration of the call.

For this option, set the following Softswitch Trunk Group Profile table tokens as follows:

- ENABLE_P_DCS_LAES_HEADER = N
- SEND_LAES_IN_RESPONSE = N
- ENABLE_ES_EVENTS = N

CALEA Operation Similar to BTS Release 4.5 with SIGNAL INSTANCE Message

To configure CALEA to operate as it did for BTS 10200 Release 4.5, with the addition of SIGNAL INSTANCE MESSAGE support, set the following ESS table tokens as follows:

Option 2:

- EM-PROTOCOL-VERSION-MAJOR = 11
- EM-PROTOCOL-VERSION-MINOR = 07
- GENERAL-PURPOSEFLAG = 1

In this configuration, the BTS 10200 does not send the P-DCS-LAES header and ignores the receipt of the P-DCS-LAES header. The BTS also disables the sending of all the new messages defined only in PacketCable 1.5 specifications (which include, REDIRECTION, CONFERENCE PARTY CHANGE, SURVEILLANCE STOP). The BTS also disables the Electronic Surveillance Indication attribute in the Signaling Start message. Furthermore, the BTS 10200 does not attempt to forward the surveillance responsibility towards the terminating party in call-forwarding situations, assuming that the forwarding party remains in the call path for the duration of the call.

For this option, set the following Softswitch Trunk Group Profile table tokens as follows:

- ENABLE_P_DCS_LAES_HEADER = N
- SEND_LAES_IN_RESPONSE = N
- ENABLE_ES_EVENTS = N

CALEA Operation According to PacketCable 1.5 Specification

To configure the CALEA feature to operate according to the PacketCable 1.5 specifications, set the following ESS table tokens as follows:

Option 3:

- EM-PROTOCOL-VERSION-MAJOR = 11
- EM-PROTOCOL-VERSION-MINOR = 07
- GENERAL-PURPOSEFLAG = 0

In this configuration, the BTS 10200 sends the P-DCS-LAES header and processes the receipt of the P-DCS-LAES header based on configuration options specified by various flags in the Softswitch Trunk Group Profile (softsw-tg-profile) table. The BTS also supports of all the new messages defined only in Packet-cable 1.5 specifications (which include, REDIRECTION, CONFERENCE PARTY CHANGE, SURVEILLANCE STOP). The BTS also enables support of the Electronic Surveillance Indication attribute in the Signaling Start message. Furthermore, the BTS 10200 forwards the surveillance responsibility towards the terminating party in call-forwarding/transfer situations.

Compliance with CALEA Requirements in PKT-SP-EM1.5-I01-050128 Appendix A

Table 2-4 describes the requirements included in the PacketCable specification PKT-SP-EM1.5-I01-050128, Appendix A and indicates the level of compliance provided by the CALEA feature in Cisco BTS 10200, Release 5.0.

Note If the endpoint type is a SIP endpoint, refer to Table 2-1. The section "BTS 10200 CALEA Interaction with SIP Endpoints" section identifies caveats that pertain to the operation of CALEA with SIP endpoints.

Table 2-4 Cisco BTS 10200 Release 5.0 Compliance with PKT-SP-EM 1.5-101-050128, Appendix A

Requirement	Description	Compliance
REQ2529	The PCES event message sent to the delivery function (DF) must not affect the monotonically increasing sequence-number that appears in the Event Message header sent to the RKS.	Compliant
REQ6108	All PCES event messages must have the Event Object field in the EM Header attribute set to 1.	Compliant
REQ6109	PCES event messages must not be sent to the RKS.	Compliant
REQ6110	Intercept Access Points (for example, CMS, CMTS, and MGC) and DF must support the Radius Protocol over UDP.	Compliant
REQ6111 REQ6112	If an IAP does not receive an Accounting-Response message within the configured retry interval, it must continue resending the same Accounting-Request until it receives an acknowledgment from the DF or the maximum number of retries is reached. The IAP can drop the request after the maximum retries is reached.	Compliant
REQ6113	When a DF receives a PCES event message in a Radius Accounting-Request message from an IAP, it must send an Accounting-Response message to the IAP.	Not applicable
Section A.1, Service Instance Message		
REQ2530	If the service (call) is under surveillance, the Service Instance Event Message must be generated with all the standard required parameters and with the additional required electronic surveillance parameters.	Compliant
Section A.2, Signaling Start		
REQ2534	If the service is under surveillance as defined in requirement 8, this event message must be generated with all the standard required parameters and with the	Compliant

REQ2535	The MGC must generate, timestamp, and send this event to the DF for a terminating call under surveillance to a PSTN gateway.	Compliant
REQ2536	The MGC must timestamp this message when it sends the SS7 IAM message or transmits the dialed digits on an MF-trunk.	Compliant
REQ2537 REQ2538	For an originating call from an MTA or from a PSTN Gateway, if the MGC receives signaling notification from the terminating CMS that the call is to be intercepted but the terminating device is unable to perform the interception, the MGC must timestamp and send an additional Signaling_Start event message to the Electronic Surveillance Delivery Function before it delivers a response to the originating MTA or PSTN gateway. This Signaling_Start event message must contain the Electronic_Surveillance_Indication attribute, and the value of the Direction_Indicator attribute must be integer 2 (2=Terminating).	Compliant
REQ2539	The CMS must generate, timestamp, and send this event to the DF if the originating call from an MTA is under surveillance.	Compliant
REQ2540	The CMS must timestamp and send this event message to the DF after all translation of the dialed digits is complete, whether the translation is successful or not. This includes unroutable digits reported to the CMS (that is, partially dialed digits).	Compliant
REQ2541	The CMS must generate, timestamp, and send this event to the DF for a terminating call to an MTA under surveillance, or for a terminating call under surveillance to an MTA.	Compliant
REQ2542	The CMS must timestamp and send this event message to the Electronic Surveillance Delivery Function prior to invoking any termination features.	Compliant

REQ2534.13.1	The Electronic_Surveillance_Indication attribute must be present in events sent to the DF for terminating calls that have been redirected by a surveillance subject.	Compliant
Section A.3, Signaling Stop		
REQ6120	If the service (call) is under surveillance, this event message must be generated with all the standard required parameters and with the additional required electronic surveillance parameters.	Compliant
REQ6121	A Signaling_Stop message must not be generated unless a Signaling_Start message with the same BCID has been generated for the call.	Compliant
REQ6122	A Signaling_Stop message *must* be generated if a Signaling_Start message with the same BCID has been generated for the call (In exception cases, this may be the result of a proprietary timeout or cleanup process.)	Compliant
REQ6123	Originating CMS: In the single-zone scenario, the originating CMS must timestamp this EM message immediately upon transmission of the NCS-signaling DLCX message.	Compliant
REQ6124	Originating CMS: In the intradomain or interdomain scenario, the originating CMS must timestamp this message upon transmission of the last signaling event in the following list: • Transmission of the NCS-signaling DLCX message • Transmission of the CMSS-signaling BYE message or CANCEL message	Compliant
REQ6125	Terminating CMS: In the single-zone scenario, the terminating CMS must timestamp this EM message immediately upon transmission of the NCS-signaling DLCX message.	Compliant

Compliance with CALEA Requirements in PKT-SP-CMSS1.5-I01-050128 Section 7.7.2

Table 2-5 lists the requirements presented in the PacketCable specification PKT-SP-CMSS1.5 Section 7.7.2, Appendix D and indicates the level of compliance provided by the Enhanced CALEA feature for Cisco BTS 10200 Release 5.0.

Note The BTS 10200 does not originate a REFER message to the other CMS to transfer the call but can process the REFER message received from another CMS.

Table 2-5 ***Cisco BTS 10200 Release 5.0 Compliance with PKTCBL 1.5 CMSS Section 7.7.2, Appendix D***

Requirement	Description	Compliance
Section 7.6.1, Procedures at Originating Exchange (REFER Method)		
REQ5025	The CMS originating a REFER must include additional header parameters for P-DCS-Billing-Info, and should include the additional header parameters for P-DCS-LAES, and P-DCS-Redirect, as specified in Section 7.7.	Not applicable BTS does not originate REFER message on CMSS trunk.
Section 7.7.2, P-DCS-LAES		
REQ7454 REQ7455 REQ7456	The LAES-BCID field must always be present. The LAES-CCCID field must be present when the LAES-Content field is present. The LAES-Key field must not be included.	Compliant
REQ7457	When CMSO receives a 3XX Redirect response containing a P-DCS-LAES header in response to an INVITE, or receives a REFER request containing a P-DCS-LAES header in the Refer-To header for an active dialog, it must copy the received P-DCS-LAES header into the subsequent INVITE that is generated as a result of the REFER or Redirect.	Compliant
Section 7.7.2.2.1.1, Redirected Call Ends Early		
REQ7458	If CMSO receives a REFER request or 3XX Redirect response message as described	Compliant

	then CMSO must send a Surveillance Stop message to its local DF containing the following information: • REQ7458.1—The local BCID already assigned to the call (this is a required field in the event message header) • REQ7458.2—The remote BCID assigned by CMST and received in the P-DCS-LAES header • REQ7458.3—The call-data IP address and port of the remote DF of CMST received in the P-DCS-LAES header • REQ7458.4—An indicator specifying that both call-data and call-content surveillance are to be stopped • REQ7458.5—An indicator specifying that the local surveillance session (if active) and remote surveillance session are to be stopped	
Section 7.7.2.2.1.2, P-DCS-LAES Header Cannot Be Included in Subsequent INVITE		
Section 7.7.2.2.1.2.1, CMSO Chooses to Perform Requested Surveillance		
REQ7459	If CMSO chooses to perform the requested call-data surveillance function, it must send a Signaling-Start message to its local DF containing the following information: • REQ7459.1—The local BCID already	Compliant

	assigned to the call (this is a required field in the event message header) • REQ7458.6—The remote BCID assigned by CMST and received in the P-DCS-LAES header • REQ7459.2—The call-data IP address and port of the remote DF of CMST received in the P-DCS-LAES header	
REQ7460	If CMSO is already monitoring the call (for example, due to an outstanding lawfully authorized surveillance order on the originating subscriber) when it receives a P-DCS-LAES header, it must send a second Signaling-Start message to its local DF, containing the appropriate parameters as specified in the preceding item (REQ7459).	Compliant
REQ7461	If the P-DCS-LAES header received in the 3XX Redirect response or REFER request also indicates that call content surveillance is to be performed (in addition to call data surveillance), then CMSO must allocate a local CCCID for the call and request the CMTS of the originating line (or MG of the originating trunk if the originator is off-net) to provide a copy of the call content to the local DF.	Compliant

REQ7462	In addition to the call-data information specified in REQ7459, CMSO must include the following data in the Signaling-Start message to the local DF: • REQ7462.1—The local CCCID assigned to the call. • REQ7462.2—The remote CCCID assigned by CMST and received in the P-DCS-LAES header. • REQ7462.3—The call-content IP address and port of the remote DF of CMST received in the P-DCS-LAES header. • REQ7462.4—When the call ends, CMSO must send a Surveillance-Stop message to its local DF containing the local BCID and indicating that both local and remote call-data and call-content surveillance are to be stopped.	Compliant
Section 7.7.2.2.1.2.2, CMSO Chooses to Perform Call-Data but Not Call-Content		
REQ7463	If the P-DCS-LAES header received in the 3XX Redirect response or REFER request indicates that both call-data and call-content surveillance are to be performed, but CMSO chooses to support only call-data (and not call-content), CMSO must send a Signaling-Start	Compliant

	message to its local DF containing the call-data information specified in Section 7.7.2.2.1.2.1.	
REQ7464	CMSO must send a Surveillance-Stop message containing the following information: • REQ7464.1—The local BCID assigned by CMSO to the call. (This BCID was bound to the remote surveillance session by the previous Signaling-Start message.) • REQ7464.2—An indicator specifying that only the remote surveillance session is to be stopped. (This allows a local surveillance session that may be in progress on the originating endpoint to continue.) • REQ7464.3—An indicator specifying that (only) call-content surveillance is to be stopped. (This allows the remote call-data surveillance to continue.)	Compliant
7.7.2.2.1.2.3 CMSO Chooses Not to Perform the Requested Surveillance		
REQ7465	If CMSO chooses not to perform any of the requested surveillance functions, it must send a Surveillance-Stop message to its local DF containing the following information:	Not applicable No scenario is identified where CMSO (if BTS) chooses not

	• REQ7465.1—The local BCID assigned by CMSO to the call. (Even though the local BCID is a required parameter, it does not convey any useful information in this case, because the local BCID was not bound to the remote surveillance session by a previous Signaling-Start message.) • REQ7465.2—The remote BCID assigned by CMST and received in the P-DCS-LAES header. • REQ7465.3—The call-data IP address and port of the remote DF of CMST received in the P-DCS-LAES header. • REQ7465.4—An indicator specifying that only the remote surveillance session is to be stopped. (This allows a local surveillance session that may be in progress on the originating endpoint to continue.)	to perform the requested surveillance.
REQ7466	An indicator specifying that both call-data and call-content surveillance are to be stopped.	Not applicable No scenario is identified where CMSO (if BTS) chooses not to perform the requested surveillance.

[1] The BTS 10200 does not support sending a REFER message.

Feedback: Help us help you

Please rate this document. **Excellent** ○ ○ ○ ○ ○ **Poor**

This document solved my problem. ○ **Yes** ○ **No** ○ **Just Browsing**

Suggestions to improve this document.
(512 characters)

If you have provided a suggestion, please enter your full name and e-mail address. This information is optional and allows us to contact you if necessary.

Name

E-mail

Submit