5ESS® Switch
Law Enforcement Agency Collection Facility Interface Specification
5E14 and Later Software Releases

Document: 235-900-500
Issue Date: April 2003
Issue Number: 2.00C

Legal Notice

Copyright ©2003 Lucent Technologies, Inc. All Rights Reserved.

Notice

Every effort was made to ensure that the information in this information product was complete and accurate at the time of publication. However, information is subject to change.

This information product describes certain hardware, software, features, and capabilities of Lucent Technologies products. This information product is for information purposes; therefore, caution is advised that this information product may differ from any configuration currently installed.

This *5ESS*® switch document may contain references to the *5ESS*® switch, the *5ESS*®-2000 switch, and the *5ESS*® *AnyMedia*® Switch. The official name of the product has been changed back to the *5ESS*® switch. The documentation will not be totally reissued to change these references. Instead, the changes will be made over time, as technical changes to the document are required. In the interim, assume that any reference to the *5ESS*®-2000 switch or the *5ESS*® *AnyMedia*® Switch is also applicable to the *5ESS*® switch. It should be noted that this name change may not have been carried forward into software-influenced items such as input and output messages, master control center screens, and recent change/verify screens.

Mandatory Customer Information

Interference Information: Part 15 of FCC Rules - Refer to the *5ESS*® Switch Product Specification information product.

Trademarks

Limited Warranty

Warranty information applicable to the *5ESS*® switch may be obtained from the Lucent Technologies Account Management organization. Customer-modified hardware and/or software is not covered by this warranty.

Ordering Information

This information product is distributed by the Lucent Learning Organization (formerly, Lucent Technologies Customer Information Center) in Indianapolis, Indiana.

The order number for this information product is 235-900-500. To order, call:

1-888-LUCENT8 (1-888-582-3688) or fax to 1-800-566-9568 (from inside the continental United States)

1-317-322-6847 or fax to 1-317-322-6699 (from outside the continental United States).

Support Information

Information Product Support: To report errors or ask nontechnical questions about this or other information products produced by Lucent Technologies, contact the Lucent Technologies Learning Organization by using one of the following methods:

Use the comment form at http://www.lucent-info.com/comments/

Send e-mail to ctiphotline@lucent.com

Please include with your comments the title, ordering number, issue number, and issue date of the information product, your complete mailing address, and your telephone number.

Technical Support Telephone Numbers: For technical assistance, call Technical Support Services (TSS) at:

1-866-LUCENT8 (1-866-582-3688) (from inside the continental United States)

1-630-224-4672 (from outside the continental United States).

Technical Support Services is staffed 24 hours a day, 7 days a week.

Acknowledgment

Developed by the Lucent Technologies Learning Organization.

Comment Form

Lucent Technologies values your comments!

Lucent Technologies welcomes your comments on this information product. Your opinion is of great value and helps us to improve. Please print out this form and complete it. Please fax the form to 407 767 2760 (U.S.) or +1 407 767 2760 (outside the U.S.). Or, you may email comments to: ctiphotline@lucent.com

Product Line: 5ESS Switch
Title: Law Enforcement Agency Collection Facility Interface Specification
Information Product Code: 235-900-500
Issue Number: 2.00C
Publication Date: April 2003

(1) Was the information product:

	Yes	No	Not Applicable
In the language of your choice?			
In the desired media (paper, CD-ROM, etc.)?			
Available when you needed it?			

Please provide any additional comments:

(2) Please rate the effectiveness of the information product:

	Excellent	More than satisfactory	Satisfactory	Less than satisfactory	Unsatisfactory	Not applicable
Ease of use						
Level of detail						
Readability and clarity						
Organization						
Completeness						
Technical accuracy						
Quality of translation						
Appearance						

If your response to any of the above questions is "Less than satisfactory" or "Unsatisfactory", please explain your rating.

(3) If you could change one thing about this information product, what would it be?

(4) Please write any other comments about this information product:

. . . . . .

Please complete the following if we may contact you for clarification or to address your concerns:

Name: _____

Company/organization: _____

Telephone number: _____

Address: _____

_____

Email Address: _____

Job function: _____

1. INTRODUCTION

1.1 PURPOSE

The "*5ESS*® Switch Law Enforcement Agency Collection Facility Interface Specification" describes the technical specifications and protocols of the interface between the *5ESS*® switch and a law enforcement agency's (LEA) collection facility and is used to determine whether a given implementation of the LEA collection facility will interwork properly with the *5ESS*® switch offering.

Interface specifications are used in the design of customer premises equipment (CPE) or to establish or troubleshoot the particular interface. As such, the primary audience for this information product is any third-party vendor contracted to provide hardware/firmware/software that will interface with the *5ESS*® switch for purposes of switch-owner compliance with the Communications Assistance for Law Enforcement Act (CALEA) of 1994. The secondary audience is comprised of the actual switch owners.

1.2 UPDATE INFORMATION

1.2.1 REASON FOR UPDATE

This information product has been updated with changes to the secured feature 99-5E-8318, CALEA CDC (Call Detail Channel) with Voice Band Transmission for Software Release 5E16.2, FR1, specifically:

- Chapter 1 , Section 1.9.1 , "CALEA CCC/CDC ENHANCEMENTS"
- Chapter 1 , Section 1.11 ., "CALEA APPLICATION of GR-30"
- Chapter 2 , Section 2.1 "CALEA Requirements"
- Chapter 2 , Section 2.2.1 "Delivery to LEA"
- Chapter 2 , Section 2.2.7 "GR-30 Overview"
- Chapter 6 , "GR-30 CDC VOICEBAND DATA TRANSMISSION"
- Chapter 7 , Section 7.3.3 "CDC: Call Data Channel"

This information product has also been updated with changes to Chapter 3 , Section 3.2.3.1.2 , to further clarify the text and figures pertaining to local and remote LEA Destination DN provisioning options.

1.2.2 SUPPORTED SOFTWARE RELEASES

This information product supports the 5E14 and later software releases available on the *5ESS*® switch.

1.2.3 TERMINOLOGY

1.2.3.1 Lucent Electronic Delivery

The Lucent Electronic Delivery system is replacing the Software Change Administration and Notification System (SCANS) as the system used to download software changes to Lucent products. During the transition, both systems will be supported. When products no longer require SCANS, Lucent Technologies will notify any customers still using SCANS of the plans for completing the migration to Lucent Electronic Delivery. The *OneLink Manager ASM User's Guide*, 235-200-145, describes the Lucent Electronic Delivery System. Documentation currently referencing SCANS will be changed over time, as other technical changes are required.

1.2.3.2 Communication Module Name Change

The term Communication Module (CM) has been changed to the Global Messaging Server (GMS), representing the new portfolio name of this particular module. The current names of the specific types and the GMS (the CM2 and CM3) have not been changed. Where the CM name has been used in a generic way within this information product, the name will be changed to GMS. Where the specific version of GMS (CM2 or CM3) is being described or mentioned, the name will not be changed. However, the GMS name may be added to the description in certain places as a reminder of the change, and that the particular version is a part of the overall portfolio. The following list provides some examples of how you may see these names used together:

- Global Messaging Server (formerly Communication Module)
- GMS (formerly CM)
- Global Messaging Server-CM2
- GMS-CM2
- Global Messaging Server-CM3
- GMS-CM3

These name changes will be made over time as other technical changes are required. Also, these changes may not be reflected in all software interfaces (input and output messages, master control center screens, and recent change and verify screens). Where the information product references these areas, the names are used as they are within the software interface.

1.2.3.3 Bellcore/Telcordia Name Change

As of March 18, 1999, Bellcore officially changed its name to Telcordia Technologies. Not all pages of this document are being reissued to reflect this change; instead, the pages will be reissued over time, as technical and other changes are required. Customers on standing order for this document may see that, on previous-issue pages, the Bellcore name is still exclusively used.

Customers receiving new orders for this document will see the Telcordia Technologies name used as appropriate throughout the document, and the Bellcore name used only to identify items that were produced under the Bellcore name. Exceptions may exist in software-influenced elements such as input/output messages, master control center screens, and recent change/verify screens. These elements will not be changed in this document until such time as they are changed in the software code. Document updates will not be made specifically to remove historical references to Bellcore.

1.2.3.4 *5ESS*®-2000 Switch Name Change

This *5ESS*® switch document may contain references to the *5ESS*® switch, the 5ESS-2000 switch, and the 5ESS AnyMedia Switch. The official name of the product has been changed back to the *5ESS*® switch. The documentation will not be totally reissued to change these references. Instead, the changes will be made over time, as technical changes to the document are required. In the interim, assume that any reference to the 5ESS-2000 switch or the 5ESS AnyMedia Switch is also applicable to the *5ESS*® switch. It should be noted that this name change may not have been carried forward into software-influenced items such as input and output messages, master control center screens, and recent change/verify screens.

1.3 ORGANIZATION

This document contains the following:

(1) INTRODUCTION

(2) SWITCH TO LEA INTERFACE

(3) PHYSICAL, LINK, AND NETWORK LAYERS

(4) IP LAYER

(5) TRANSPORT LAYER - TCP

(6) APPLICATION LAYER

(7) GLOSSARY

1.4 USER COMMENTS

We are constantly striving to improve the quality and usability of this information product. Please use one of the following options to provide us with your comments:

- You may use the on-line comment form at **http://www.lucent-info.com/comments**
- You may email your comments to **ctiphotline@lucent.com**

Please include with your comments the title, ordering number, issue number, and issue date of the information product, your complete mailing address, and your telephone number.

If you have questions or comments about the distribution of our information products, see Section 1.5 , Distribution.

1.5 DISTRIBUTION

For distribution comments or questions, either contact your local Lucent Technologies Account Representative or send them directly to the Lucent Learning Organization.

A documentation coordinator has authorization from Lucent Technologies to purchase our information products at discounted prices. To find out whether your company has this authorization through a documentation coordinator, call **1-888-LUCENT8 (1-888-582-3688)**.

Customers who are not represented by a documentation coordinator and employees of Lucent Technologies should order *5ESS*® switch information products directly from the Lucent Learning Organization.

To order, call the following telephone number:

- **1-888-LUCENT8 (1-888-582-3688)** or fax to **1-800-566-9568**; from inside the continental United States
- **1-317-322-6847** or fax to **1-317-322-6699**; from outside the continental United States.

1.6 TECHNICAL ASSISTANCE

For technical assistance, call Technical Support Services (TSS) at:

- **1-866-LUCENT8 (1-866-582-3688)**; from inside the continental United States
- **1-630-224-4672**; from outside the continental United States.

Technical Support Services is staffed 24 hours a day, 7 days a week.

1.7 REFERENCES

The following is a list of other documents that are referred to in this document.

- 235-900-341, *5ESS® Switch National ISDN Basic Rate Interface Specification*
- 235-900-343, *5ESS® Switch Custom ISDN Basic Rate Interface Specification*
- J-STD-025/J-STD-025 Revision A, Lawfully Authorized Electronic Surveillance.
- T1.260-1998, the industry standard for the administrative interface
- RFC 791, Internet Protocol
- RFC 792, Internet Control Message Protocol
- RFC 793, Transmission Control Protocol
- RFC 1122, Requirements for Internet Hosts-Communications Layers
- ITU-T (formerly CCITT) Recommendation X.25 (1984), Interface Between DTE and DCE (for terminals operating in the packet mode and connected to public data networks by dedicated circuit)
- ITU-T (formerly CCITT) Recommendation X.208, Abstract Notation One (ASN.1)
- ITU-T (formerly CCITT) Recommendation X.209, Basic Encoding Rules
- Telcordia GR-30-CORE, Issue 2, "Voiceband Data Transmission Interface", December, 1998.
- Telcordia GR-506-CORE, "Lawful Access Feature: Switching Generic Requirements Access to Call-Identifying and Call Content Information", Issue 4, April 2000.
- American National Standards Institute, T1.401-1993, "Interface Between Carriers and Customer Installations - Analog Voicegrade Switched Access Lines Using Loop-Start and Ground-Start Signaling", August 18, 1993.
- American National Standards Institute, T1.401.3-1998, "Network-to-Customer Installations Interfaces - Analog Voicegrade Switched Access Lines with Calling Number Delivery, Calling Name Delivery, or Visual Message-Waiting Indicator Features", June 9, 1998.

1.7.1 STANDARDS COMPLIANCE

NOTE: The CALEA application complies with ITU-T X.25 DCE specifications. TCP/IP/X.25 complies to the delivery specifications documented in Telecommunications Industry Association document, "Lawfully Authorized Electronic Surveillance," J-STD-025 and J-STD-025 Revision A. The Core TCP/IP Suite Functionality feature makes this interface compliant with respect to IP version 4 (IPv4).

1.8 DEFINITION OF TERMS

Definitions of the commonly used terms in this document are as follows:

Associate	A subscriber whose equipment, facilities, or services are communicating with a subject. The redirected subscriber becomes an "associate" and may be "monitored" as a "subject".
Blocking	The inability of the calling party to be connected to the called party because all suitable

trunk paths are busy, or a path between a given inlet and any suitable free outlet of the switch is unavailable.

C-Tone — A single-frequency Continuity Tone (480 Hz) may be applied to a CCC channel connected to an LEA when the channel is assigned to a surveillance but not connected to an active call. C-Tone is removed when the CCOpen is sent and is applied when the CCClose is sent. C-Tone is provisionable on a per-switch basis.

Prior to 5E16.2, the *5ESS*® switch used High Tone as C-Tone. In 5E16.2, the *5ESS*® switch will have an office option to use either High Tone, DTMF C-Tone or silence as the C-Tone.

CALEA — Communications Assistance for Law Enforcement Act.

Call Content — This refers to call content being delivered to the LEA via a CCC (call content channel that carries circuit-switched data and voice) or PDC (packet data channel that carries packet-switched data). For voice calls, it is the voice transmission to and from a subject. For data calls, it is the data being received and transmitted by a subject. For packet calls, it is the packets being received and transmitted by a subject.

Call Content Channel (CCC) — A transmission path used to deliver call content to the LEA. Circuit CCCs are used for monitoring circuit-switched voice (CSV) and circuit-switched data (CSD) calls. Note that the Bellcore Standard version of a CCC corresponds to Lucent's PDC (carries packet data) and CCC (carries circuit-switched data).

Call Data — Information regarding the intercept subject and call-identifying information for circuit-switched and packet-switched calls.

Call Data Channel (CDC) — The logical link between the device performing a surveillance access function and the LEA that carries information regarding the intercept subject and call-identifying information for circuit-switched and packet-switched calls.

Call Identity — An alpha-numerical call identification value which has been obtained and allocated by the switch to identify messages associated with a particular call under surveillance. Each call (call leg for redirected calls) gets a unique per-switch call identity value.

Call Progress Data — The dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber through any equipment, facility, or service of a telecommunications carrier. This phrase is synonymous with "call-identifying information".

CaseIdentity — A 25-character identifier used in CDC messages, assigned by an LEA for a particular surveillance at the time of provisioning of the surveillance.

CCClose — A message used to report the end of call content delivery on the Call Content Channel (CCC) and on the Packet Data Channel (PDC).

CCOpen — A message used to report the beginning of call content delivery on the Call Content Channel (CCC) and on the Packet Data Channel (PDC).

Cut Through — The point in call setup when a transmission path is established between the calling and called party.

DTMF-C Tone — DTMF-C Tone is one of the office options that can be used as the C-Tone. It is a dual frequency tone defined as:

- Frequency 1: 1633 Hz = or - 1.5%

- Frequency 2: 852 Hz = or - 1.5%
- Tone Level 1: -7 dBm + or - 1dB
- Tone Level 2: -7 dBm + or - 1dB

High Tone — High Tone is one of the office options that can be used as the C-Tone. It is a single frequency tone of 480 Hz at -17dB.

Intercept Access Point (IAP) — A point within a service provider's network where call content or call progress data is accessed.

IAP switch — A switch upon which a given intercept subject DN is homed. It is synonymous with "subject switch".

laesCaseIdentity — The administrative attribute specifying CaseIdentity. The laesCaseIdentity may represent one or more surveillances.

laesCase — The administrative object containing attributes related to a network-based surveillance.

laesCaseNameID — Identifies a specific instance of an laesCase. There may be multiple laesCaseNameIds associated with one laesCaseIdentity.

Law Enforcement Agency (LEA) — A government entity with the legal authority to conduct an electronic surveillance.

Level of Surveillance — Specifies the nature of the call content and/or call progress data to be identified and collected.

Monitor — To provide information about activity associated with a subject. This may be call progress data only (Level I surveillance) and/or actual call content (Level II surveillance).

Monitoring Station — An LEA facility for collecting call data and, for Level II Surveillances, call content.

Packet Data Channel (PDC) — A path used to deliver packet-switched call content to the LEA.

Redirection — A call leg, involving an intercept subject or controlled on behalf of an intercept subject, is rerouted to another call leg (DN or announcement). The intercept subject no longer has control over the call.

Subject — The equipment, facilities, or services of a subscriber whose incoming, outgoing, and redirected communications and/or call-identifying information is to be accessed and delivered to law enforcement pursuant to a court order or lawful authorization.

Subject DN — A directory number designated for surveillance.

Subscriber — A residential or business telephone customer who may be identified by a lawful court order as a "subject" under surveillance.

Surveillance — The process of continuously accessing specified call content and/or content/data to a specified remote law enforcement agency over a specified period of time.

Surveillance Administration System (SAS) — The entity that sends messages to a switch to establish, maintain, and discontinue surveillances. A SAS may be a person, who manually sends surveillance administration messages or a complex system that provides an automated interface to a number of Intercept Access Point switches.

Surveillance Administration Interface (SAI) The logical link that carries surveillance administration messages between the Surveillance Administration System and the Intercept Access Point switch.

Surveillance Profile A set of attributes specifying for a surveillance whether that surveillance is Level I surveillance or a Level II surveillance, and which CDC messages (and parameters within those messages) are allowed to be sent to the LEA.

Switch Access Point The hardware connection point within the Intercept Access Point Switch that provides access to call content.

SM Switching module. Since the CALEA application is deployed in all SMs and SM-2000s, any occurrence of the terms SM or SMP (switching module processor) throughout this information product refers to both the SM and SM-2000.

Tainted Call A call that was redirected by a subject and the subject is no longer part of the call.

1.9 WHAT IS CALEA?

The Communications Assistance for Law Enforcement Act (CALEA) Core feature (99-5E-4275) in the 5E14 software release provides compliance to the Communications Assistance for Law Enforcement Act (CALEA) of 1994 for *5ESS*® switches providing service to wireline subscribers.

CALEA requires that a telecommunications service provider be able to support lawful surveillance of the traffic in its network.

The CALEA Punchlist feature, 99-5E-7599, provides compliance to the additional capabilities mandated by the Department of Justice. J-STD-025A provides the additional requirements for the interface between the TSP and the LEA.

1.9.1 CALEA CCC/CDC ENHANCEMENTS

The CALEA Enhancement for Dial Out CDC and CCC feature, 99-5E-8221, provides alternate provisioning as an enhancement to the CALEA-CORE feature (99-5E-4275). This enhancement uses Dial Out CDC and CCC connections whenever the subject makes or receives a call.

The CALEA CDC with Voice Band Data Transmission, feature 99-5E-8318, is an enhancement to the CALEA Dial Out CDC and CCC feature (99-5E-8221). This enhancement allows the CDC messages to be transmitted over an analog line termination.

After the enhancements made in 5E16.2, *5ESS*® supports the following possible CCC and CDC interfaces:

CCC interface:

- Dedicated CCC (by 99-5E-4275 in 5E14.1)
- Dial out CCC (by 99-5E-8221 in 5E16.2)

CDC interface:

- TCP/IP over PVC (by 99-5E-4275 in 5E14.1)
- TCP/IP over SVC (by 99-5E-8221 in 5E16.2)
- Voice Band Data Transmission GR-30 (by 99-5E-8318 in 5E16.2)

1.10 CALEA APPLICATION USE OF TCP/IP

1.10.1 TCP/IP ACCESS PROTOCOLS

The "Core TCP/IP Access via X.25" feature allows a Core TCP/IP Platform application on the *5ESS*® switch to interface with a remote host (an LEA collection facility containing up to 5 monitoring stations) over a basic rate interface (BRI) or T1, using LAPB as the Layer 2 protocol, IP over X.25 as the Layer 3 protocol, and TCP as the Layer 4 protocol. For the X.25 interface, the switch will act as the Data Circuit Terminating Equipment (DCE) while the LEA collection facility will act as the Data Terminal Equipment (DTE). Permanent Virtual Circuits (PVCs) will be utilized.

NOTE: While there is a limit of 5 monitoring stations per collection facility, the switch itself can support up to a total of 48 monitoring stations.

Switched Virtual Circuits (SVCs) are supported, as of software release 5E16.2. The SVC is originated by the switch on a newly supported PSUEN XAT interface to the X.25 packet destination on the C.4 laescase view. The X.25 SVC packet call may be routed over an X.25, XAT T1 X.75 or X.75' interface to reach the remote host.

The core protocol suite includes the Transmission Control protocol (TCP), the Internet Protocol Version 4 (IPv4), and a subset of the Internet Control Message Protocol (ICMP). These protocols will evolve as the standards for the protocols evolve.

The "Dial Out CDC and CCC CALEA Enhancement" feature provides alternative provisioning as an enhancement to the "CALEA-CORE feature. This enhancement uses a dial out CDC and CDC connection whenever the subject makes or receives a call. For CDC dial out, a Switched Virtual Circuit (SVC) connection will be established from an XAT PH Channel Group Member emulating an X.25 DTE to a local LEA via a BRI or XAT termination. The SVC can also be established from the emulated X.25 DTE to a remote LEA via X.75 or X.75' packet network. For CCC, the connection will be established to the destination LEA via call forwarding on the Local LEA CCC DN (from C.4). The destination LEA may be a local POTS or ISDN termination or a remote termination via SS7, PRI, or MF trunk(s). The CCC connection can also be established to a remote LEA over an SS7 or MF trunk over the public switched telephone network. This feature supports combined. separated, or mixed CCC transmit and received delivery modes.

1.10.2 TCP/IP INTERFACES AND THEIR PAYLOAD

In the 5E14 software release, the CALEA application requires the use of TCP/IP/X.25/LAPB/BRI, TCP/IP/X.25/LAPB/XAT, TCP/IP/X.75/LAPB/T1, and TCP/IP/X.75'/LAPB/T1 interfaces to transport Call Data Channel (CDC) messages and Packet Data Channel (PDC) packets from the switch to LEA monitoring stations.

In the 5E16.2 software release, TCP/IP and PSUEN XAT interfaces are available to transport CDC messages, not PDC using X.25 SVC connections.

NOTE: Only an X.25 BRI B-channel or XAT can be connected to the LEA collection facility. X.75/X.75' trunks may be part of an overall data network, but are never physically connected to an LEA collection facility, therefore, X.75/X.75' trunks are outside the scope of this document.

The CDC messages are generated in the Switching Module Processor (SMP) while the PDC packets are generated in the subject's Packet Handler (PH). These are encapsulated into TPKT headers and TCP/IP messages and sent via IP routing to the PH that serves the interface between the switch and the LEA (that is, the delivery PH).

NOTE: The CALEA-Core TCP/IP feature has been developed for the PH3 and PH4 ISDN images with channel type DSLG, ISM, X.75, and X.75'.

In the delivery PH, the TCP/IP messages are encapsulated into X.25 messages, as determined by

provisioning, and transported over an ISDN X.25/XAT permanent virtual circuit (PVC) to reach the designated LEA.

For the basic rate interface (BRI), PVCs are assigned to the B-channel. Recent Change/Verify (RC/V) for the CALEA-Core feature will block provisioning of the PVC to the D-channel.

1.10.3 SIGNALING RATES

The dedicated BRI consists of two 64-kbps B-channels to support circuit-switched data (CSD) and packet-switched data (PSD) services. The dedicated XAT interface supports a provisionable signaling rate of either 56 kbps or 64 kbps.

1.11 CALEA APPLICATION USE of GR-30

The "CDC with Voice Band Data Transmission" feature provides the ability to provision an analog line termination to transmit CDC messages. This is an enhancement to the "Dial Out CDC and CCC" feature. This enhancement allows service providers to setup a CDC connection to a local LEA using an analog line termination. A CDC connection can also be established from the analog line termination on the switch to a remote LEA over an ISUP or MF trunk via the public switched telephone network. Service providers can provision CDC surveillances quicker and with less cost than dedicated trunk surveillances. The CDC analog link interface supports a signaling rate of 1200 bits/seconds (bps), which is sufficient for a small number of surveillances. Multiple surveillances can use the same analog CDC connection to an LEA. The CDC messages are sent using GR-30 FSK signaling.

2. SWITCH TO LEA INTERFACE

2.1 CALEA REQUIREMENTS

Available in the 5E14 software release, the three-feature set composed of the CALEA - Core feature (99-5E-4275), the CALEA Core TCP/IP DSL Access via X.25 feature (99-5E-4908), and the CALEA Core TCP/IP Functionality and API feature (99-5E-4907), provides compliance to the Communications Assistance for Law Enforcement Act (CALEA) of 1994 for *5ESS*® switches providing service to wireline subscribers.

CALEA requires that a telecommunications service provider be able to support two levels of lawful surveillance of the traffic in its network.

- Level I: Provides call progress data for all of the subject's calls and call progress data for all calls redirected by the subject. Call content is not provided. This level is intended to satisfy Pen Register as well as Trap and Trace court orders.

- Level II: Provides call progress data and all call content. It is equivalent to Level I plus call content. This is intended to satisfy a Title III court order that specifically authorizes the surveillance of call content for the subject's calls and for all calls redirected by the subject.

The feature set provides functionality for both circuit-switched and packet-switched calls in accordance with Standard J-STD-025, *"Lawfully Authorized Electronic Surveillance"*, authored by the Telecommunications Industry Association (TIA) TR45.2 subcommittee. Refer to J-STD-025, Annex A, *"Deployment Examples"*,*"A.5 Possible CDC Protocol Stacks"*, option "d".

The feature set includes the *5ESS*® switch functionality necessary to access and deliver call data and call content to a Law Enforcement Agency and the functionality necessary to administer surveillances and provision and maintain call content channels (CCCs), call data channels (CDCs), and packet data channels (PDCs).

Note that Bellcore standards definition of a CCC covers both circuit- and packet-switched call content and is equivalent to Lucent Technologies' two channels: PDC (carries only packet-switched call content) and CCC (carries only circuit-switched call content).

Feature 99-5E-7599, CALEA Punchlist (the second phase of Lucent's CALEA application in the 5E15 software release), provides compliance with the additional requirements mandated by the government via the J-STD-025A ballot copy.

Figure 2-1 provides an overview of the CALEA network, including the SAS, the switch, and the LEA collection facility interfaces.

Figure 2-1 CALEA Network Block Diagram

As part of the Call Content Channel maintenance, C-Tone is optional and is provisionable per office. C-Tone is an idle circuit continuity tone on each idle Call Content Channel connecting the switch to a Law Enforcement Agency.

The CALEA Enhancement for Dial Out CDC and CCC feature (99-5E-8221) provides alternative provisioning as an enhancement to the CALEA-CORE feature (99-5E-4275). This enhancement uses Dial Out CDC and CCC connections whenever the subject makes or receives a call.

For Dial Out CDC , the capability of using Switched Virtual Circuits (SVCs) to send CDC (not PDC) messages to law enforcement collection facilities is added. The SVC connection will be established from an XAT PH logical channel emulating an X.25 DTE to a local LEA facility via a BRI or XAT termination. The SVCs are originated on a XAT PH channel group member (Packet Switching Unit Equipment Number - PSUEN) where by the *5ESS*® switch emulates a DTE to establish the X.25 packet call. The destination address of the X.25 packet call originated by the emulated DTE can route using the local packet network or X.75/X.75' network. The X.25 destination address is specified by the application. Note that X.25 SVC packet standards are supported on local (BRI/XAT) and X.75/X.75' interfaces.

For Dial Out CCC , the connection will be established to a local LEA with POTS or ISDN BRI/PRI termination. The CCC connection can also be established to a remote LEA over SS7, MF or PRI trunks over the public switched telephone network. This feature supports combined, separate and mixed delivery modes.

The CALEA CDC with Voice Band Data Transmission feature (99-5E-8318) provides the ability to provision

an analog line termination to transmit CDC messages. This is an enhancement to the "Dial Out CDC and CCC" feature. This enhancement allows service providers to setup a CDC connection to a local LEA using an analog line termination. A CDC connection can also be established from the analog line termination on the switch to a remote LEA over an ISUP or MF trunk via the public switched telephone network. Service providers can provision CDC surveillances quicker and with less cost than dedicated trunk surveillances. The CDC analog link interface supports a signaling rate of 1200 bits/second (bps), which is sufficient for a small number of surveillances. Multiple surveillances can use the same analog CDC connection to an LEA.

2.2 LEA INTERFACE

2.2.1 DELIVERY TO LEA

Surveillance delivery capabilities are responsible for transporting call content and call progress data from the subject's switch to law enforcement monitoring sites. Delivery capabilities perform the following functions:

- establish and maintain delivery channels to monitor location,
- format generated surveillance data into call processing messages, and
- deliver call data messages and call content.

NOTE: The *5ESS*® switch acts as the "client", while the LEA monitoring facility acts as the "server".

Circuit-switched call content data is delivered over a CCC pair. A CCC dedicated trunk circuit has only one intercept subject assigned to it. Additional dedicated trunk circuits are required for each subject and LEA. All trunk circuits within a CCC trunk group will terminate to the same LEA collection facility.

The dial out CCC uses a local LEA DN to set up a transmission path to the LEA collection facility. Circuit-switched call content is delivered in one of three modes; separate, combined , or mixed. The combined CCC option uses one channel for transmit and receive call content. The mixed CCC option uses a combined channel if the bearer capability of the intercepted call is "speech" or "3.1 audio" , and it will use separated channel for any other bearer capabilities. The dial out CCC line terminates to the same LEA collection facility, or is routed to a remote office via PSTN. Currently, dial out CCCs does not support multiple LEAs for the same subject.

Packet-switched call content data is delivered over a PDC (a dedicated X.25 packet switching access on T1 facilities (XAT)/ basic rate interface (BRI) X.25 PVC to the Law Enforcement Agency monitoring station).

Call detail data is delivered over CDC via TCP/IP over X.25. Call content for packet calls is delivered over PDC via TCP/IP over X.25. Circuit-switched call content data is delivered over a CCC.

NOTE: For software release 5E16.2, CALEA Enhancement Support Multiple LEA for CCC Dial Out feature 99-5E-8316 provides the capability for two LEAs to monitor the same subject using the combined or separated CCC delivery mode..

Call detail data can also be sent over a CDC that uses an analog line termination. In this case, GR-30 FSK signaling is used to deliver the messages to the LEA.

2.2.2 TCP/IP OVERVIEW

An application on the switch needs to communicate with a remote host (in this case, the law enforcement agency's collection facility). TCP provides the reliable transport to get the information to the collection facility. IP provides the routing between the switch and the collection facility.

NOTE: The sockets for the CALEA application do not expect data from LEA and, as such, the receive component of the socket is closed.

The BRI provides the transmission medium for IP from the switch to the LEA collection facility attached to the BRI. The service provider must configure the interface to be consistent with the switch configuration for all layers of the interface.

The switch interfaces with the collection facility over a BRI (2B+D) or T1 (24 DS0 rate channels), using LAPB as the Layer 2 protocol and X.25 as the Layer 3 protocol. For the X.25 interface, the switch will act as the Data Circuit Terminating Equipment (DCE) while the collection facility will act as the Data Terminal Equipment (DTE). Permanent Virtual Circuits (PVCs) will be utilized. . See Figure 2-2 for a diagram of the complete protocol stack. This protocol stack adheres to option "d" of Standard J-STD-025, Annex A, *A.5 "Possible CDC Protocol Stacks"*. Switched Virtual Circuits (SVCs) are now supported for software release 5E16.2. For a diagram of the CDC Dial Out SVC Protocol Stack, see Figure 2-3

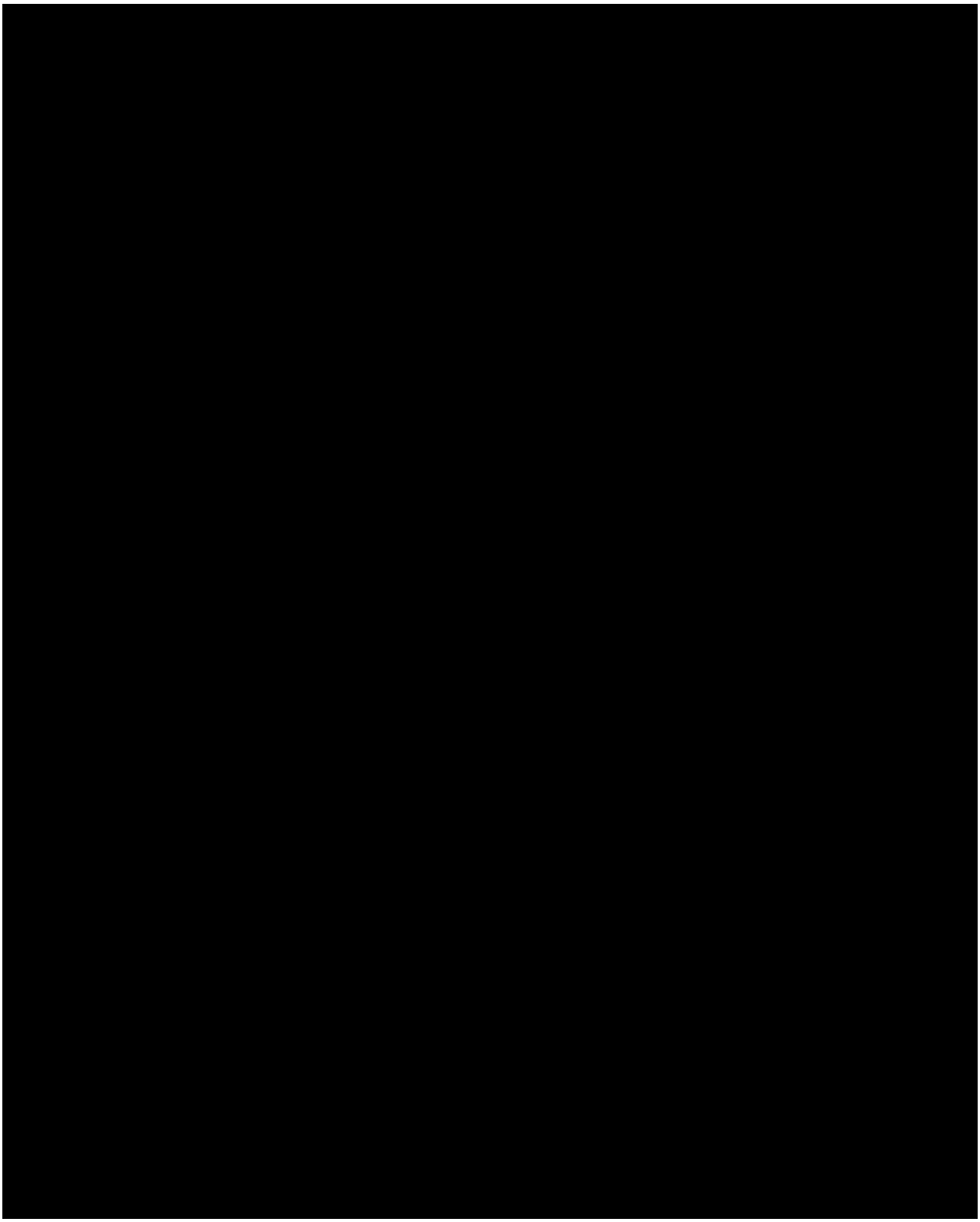

Figure 2-2 Protocol Stack

Figure 2-3 CDC Dial Out SVC Protocol Stack

Figures 2-4 , 2-5 , 2-6 , and 2-7 represent examples of connections between the switch and the LEA monitoring station.

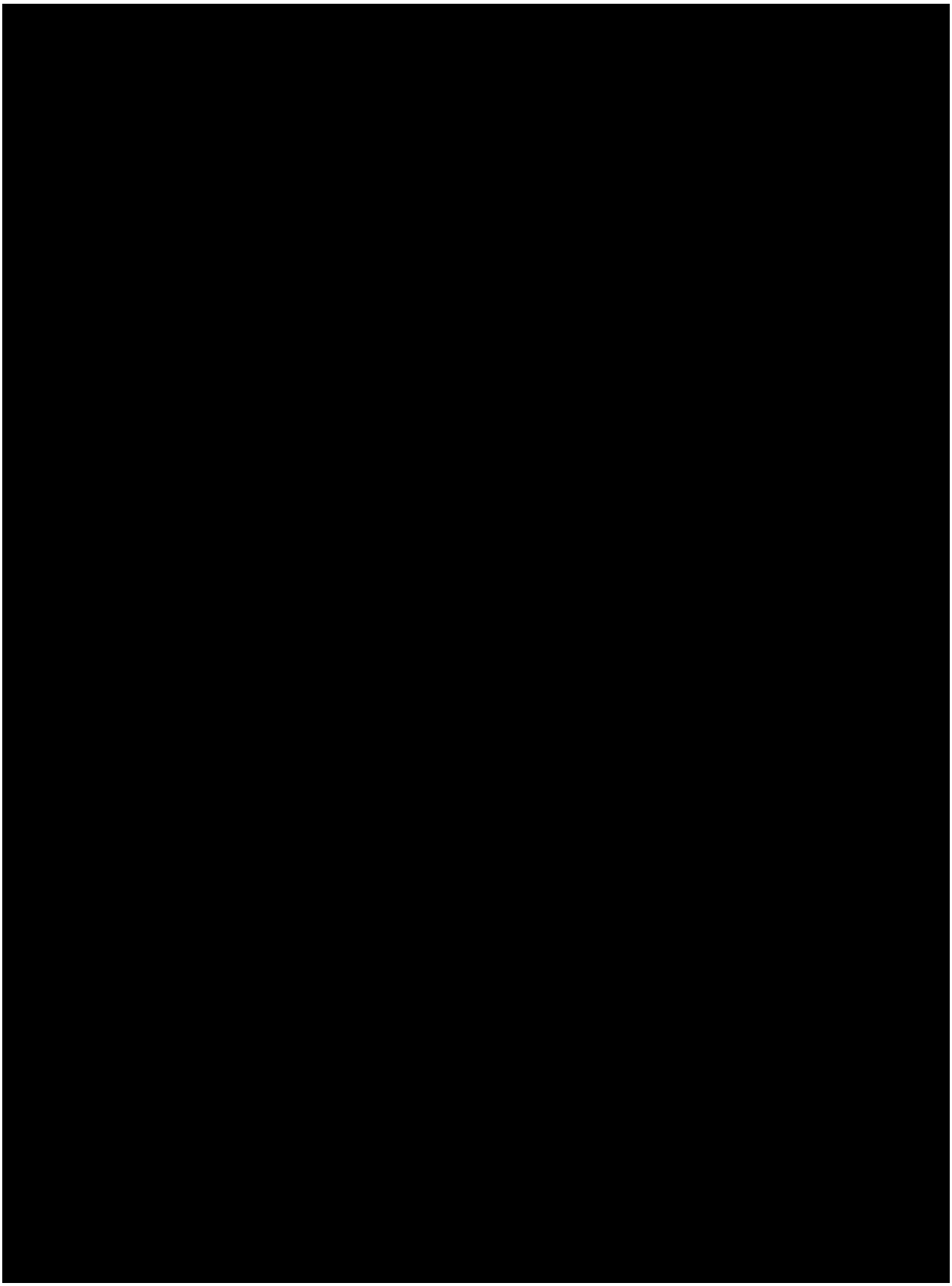

Figure 2-4 Examples of BRI Directly Connected to a Host

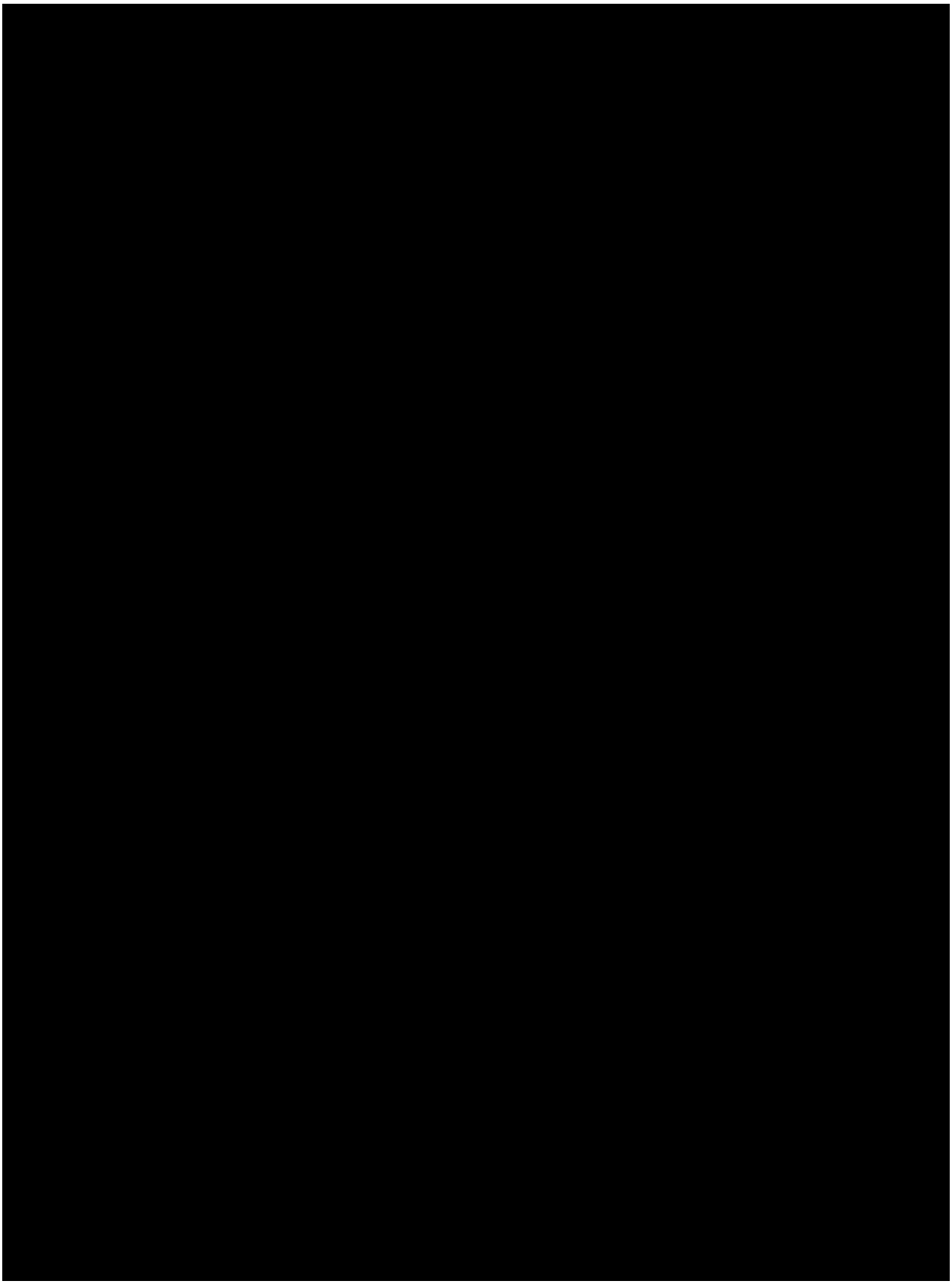

Figure 2-5 Examples of BRI Indirectly Connected to a Host

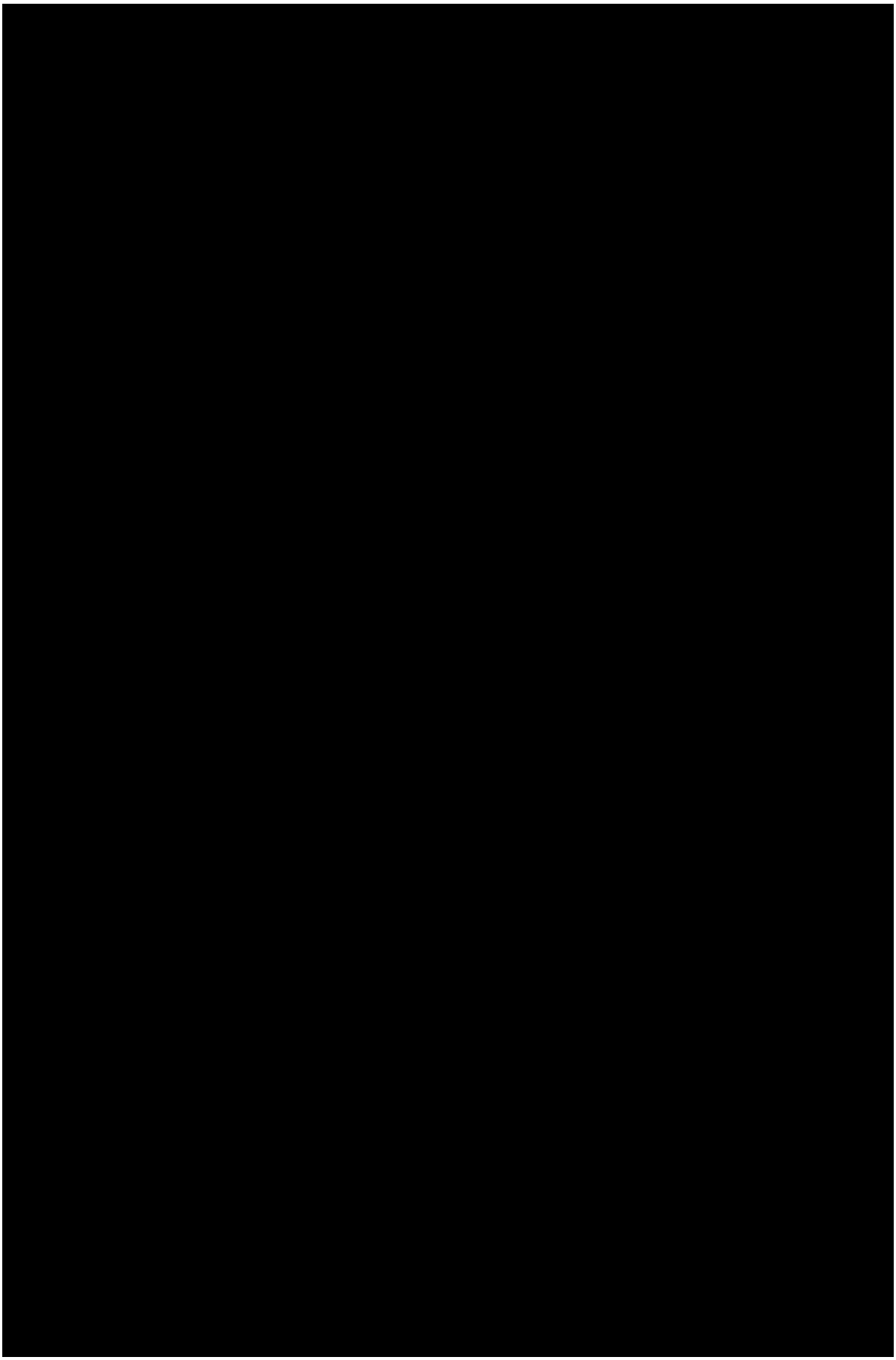

Figure 2-6 Examples of Protocol Layers - BRI Directly Connected to a Host

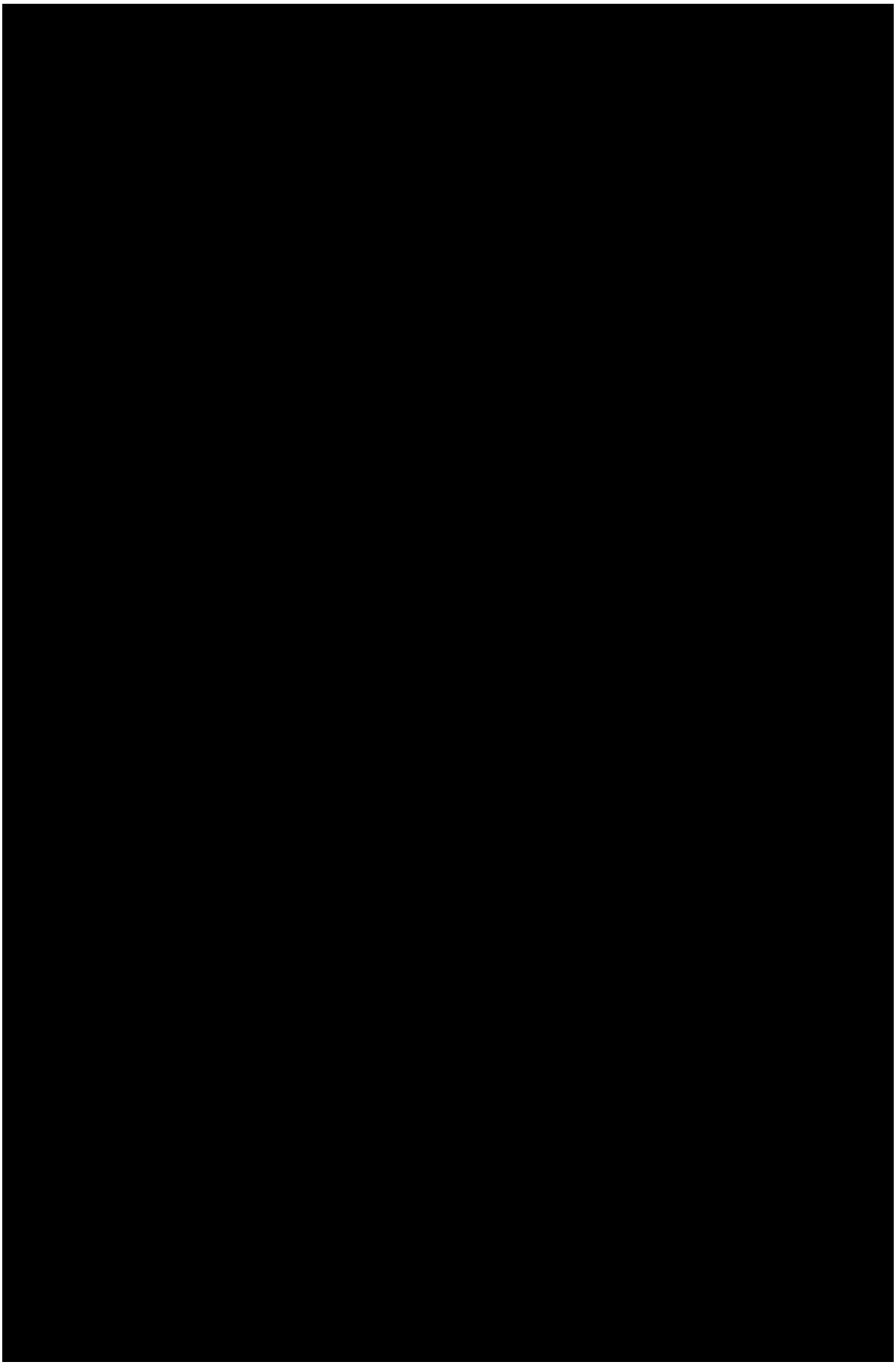

Figure 2-7 Examples of Protocol Layers - BRI Indirectly Connected to a Host

2.2.3 SOCKET CONNECTIVITY

For each level I and II circuit and packet surveillance, the LEA collection tool will expect to receive upon insertion of a Laes Case on RC/V C.4, 'n' simultaneous socket connections from the switch (clients) to the collection tool (server) where 'n' represents the number of SMs found on the *5ESS*® switch. For example, if the switch contains three SMs, upon insertion of the Laes Case there will be three simultaneous socket connections established on the collection tool for the same destination IP address and TCP port. For a level II packet surveillance, upon activation of the LAES Case, there will be two simultaneous socket connections establishing for each packet service under surveillance. For example, if the ISDN subject under surveillance has a D-channel and B1-channel packet services, four socket connections (transmit and receive sockets for the D-channel and transmit and receive socket for the B1-channel) will establish on the collection tool. Due to the collection tool acting in the capacity as a server to all socket connections from the switch, the server process or processes will need to be started before insertion of the surveillances begins via recent change. See Figure 2-8 for a graphical representation of multiple socket connections.

Figure 2-8 currently displays IP connectivity from PH INET directly to the router. In Software Release 5E16.2, Dial Out CDC and CCC feature, there may be a different PH that connects to the BRI via a SVC X.25 packet call. See Figure 2-9 for a graphical representation of the SVC connection case.

NOTE: Figure 2-9 is a detail of one SM in Figure 2-8 , illustrating an SVC connection case and impact per Dial Out CDC and CCC feature.

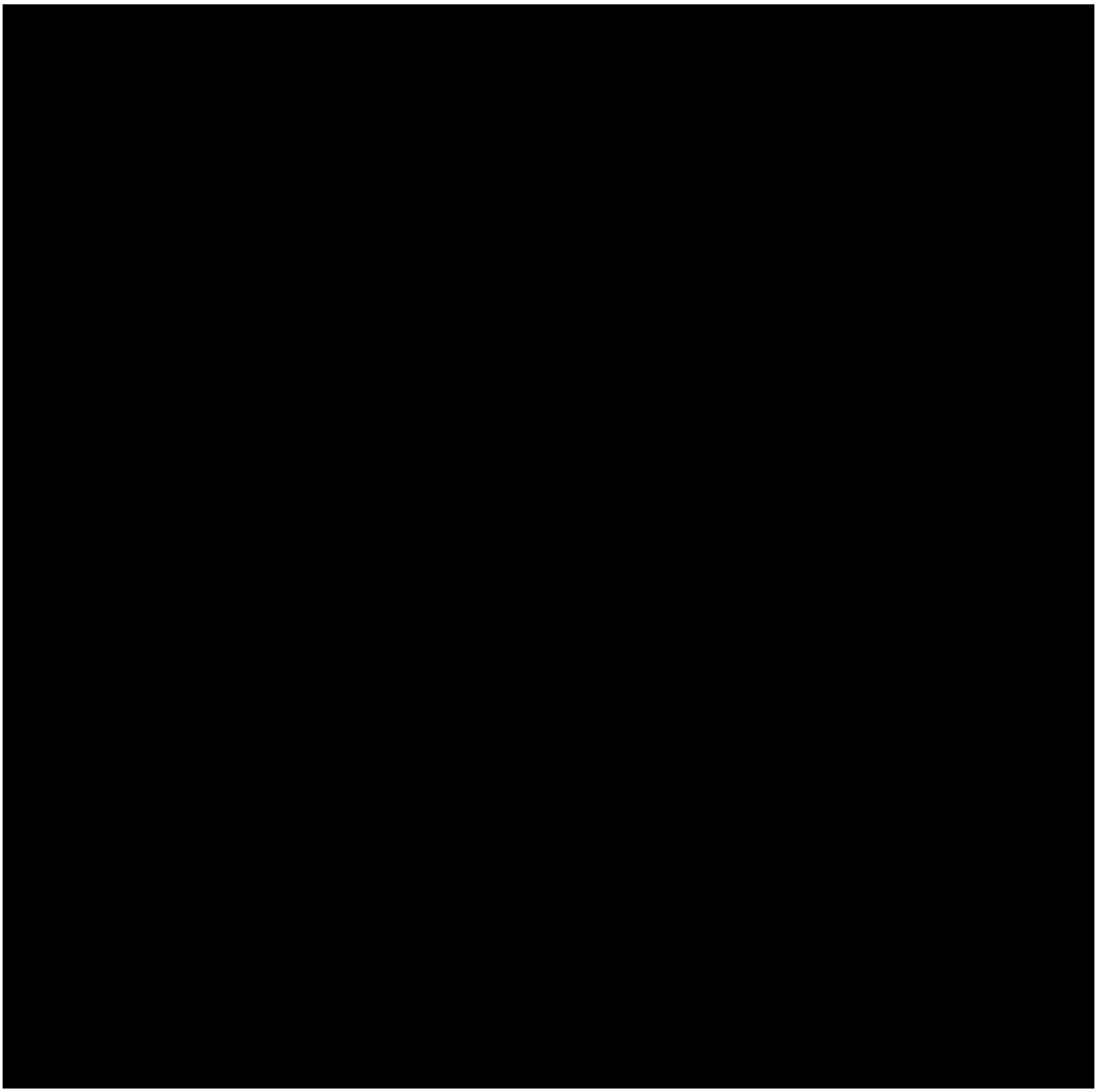

Figure 2-8 Multiple Socket Connectivity

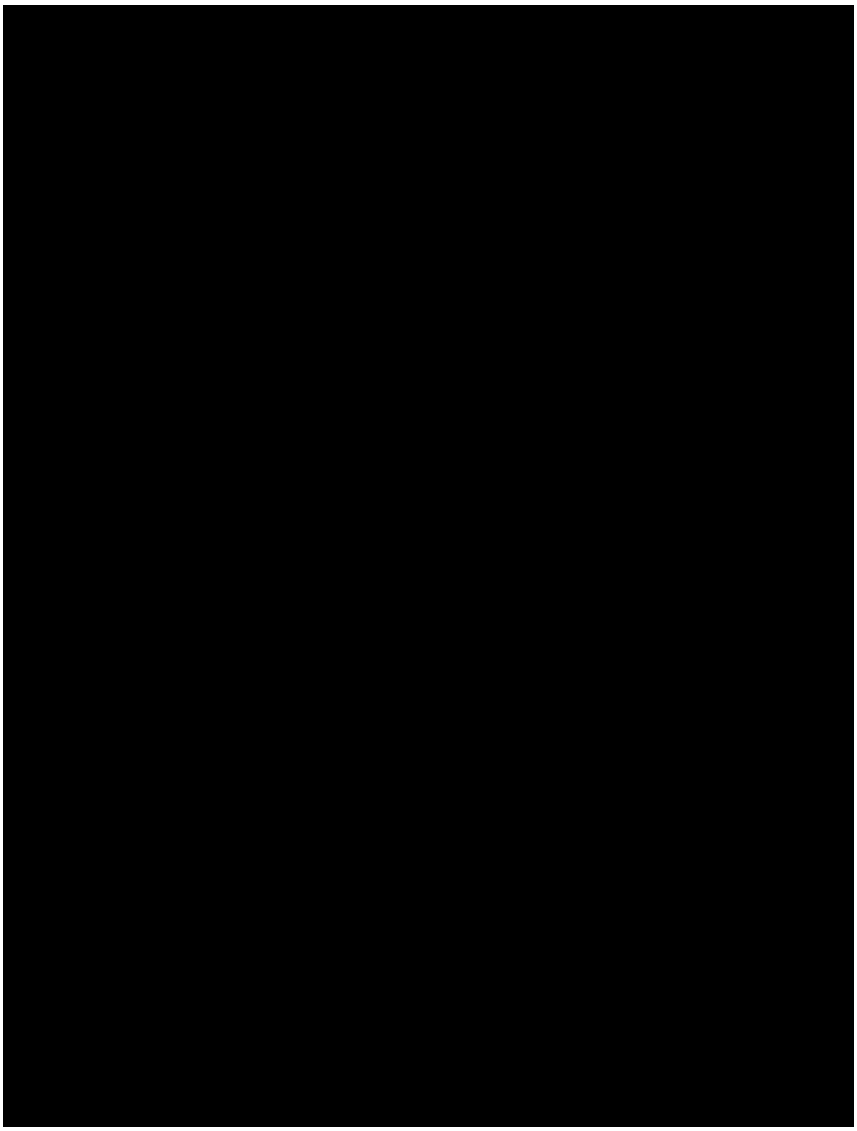

Figure 2-9 Dial Out CDC and CCC - SVC Connection Case

2.2.4 TCP/IP INTERFACES AND THEIR PAYLOAD

In the 5E14 software release, the CALEA application requires the use of:

- TCP/IP/X.25/LAPB/BRI [BRI with PPB1/PPB2 X.25 permanent virtual circuit (PVC)]
- TCP/IP/X.25/LAPB/XAT [XAT (X.25 access on a T1) PVC]

interfaces to transport Call Data Channel (CDC) messages and Packet Data Channel (PDC) packets from the switch to Law Enforcement Agency Monitoring Stations. The CDC messages are generated in the Switching Module Processor (SMP) while the PDC packets are generated in the subject's Packet Handler (PH). These are encapsulated into TCP/IP messages and sent via IP routing to a PH, which serves the interface between the switch and the Law Enforcement Agency (that is, delivery PH).

NOTE: The CALEA-Core TCP/IP feature has been developed for the PH3 and PH4 ISDN images with channel type of DSLG, ISM, X.75 and X.75'.

Each SMP and each PH has its own unique IP address within the switch.

NOTE: CALEA is supported on both National and Custom ISDN.

In the delivery PH, the CALEA Core TCP/IP Access via X.25 feature provides the software to encapsulate the TCP/IP messages into X.25 messages, as determined by provisioning, and transport these messages over the ISDN X.25 PVC or XAT PVC to the designated Law Enforcement Agency. For the BRI interface, PVCs may be assigned to the B-channel. RC/V for this feature will block provisioning of the PVC to the D-channel.

The X.25 data packets carry TCP/IP information (IP datagrams) for CDC messages and PDC packets.

Figure 2-10 illustrates the terms frame, packet, datagram, message, and segment.

Figure 2-10 Terminology Illustration

In the 5E16.2 software release, the CALEA application also supports the use of TCP/IP/X.25 SVC connections originated on a PSUEN XAT packet interface for transporting CDC messages.

Figure 2-11 illustrates the generation of CDC messages in the SMP by the CALEA application. The messages are encapsulated by the Core TCP/IP software located in the SMP, relayed to the delivery PH for transmissions to the appropriate PSUEN XAT PH channel group member, and delivered over the SVC (X.25 network) to the BRI/XAT interface where the Law Enforcement Agency (LEA) is served directly by the subject's switch.

NOTE: The PSUEN XAT and BRI/XAT serving the LEA can be on the same or different PH.

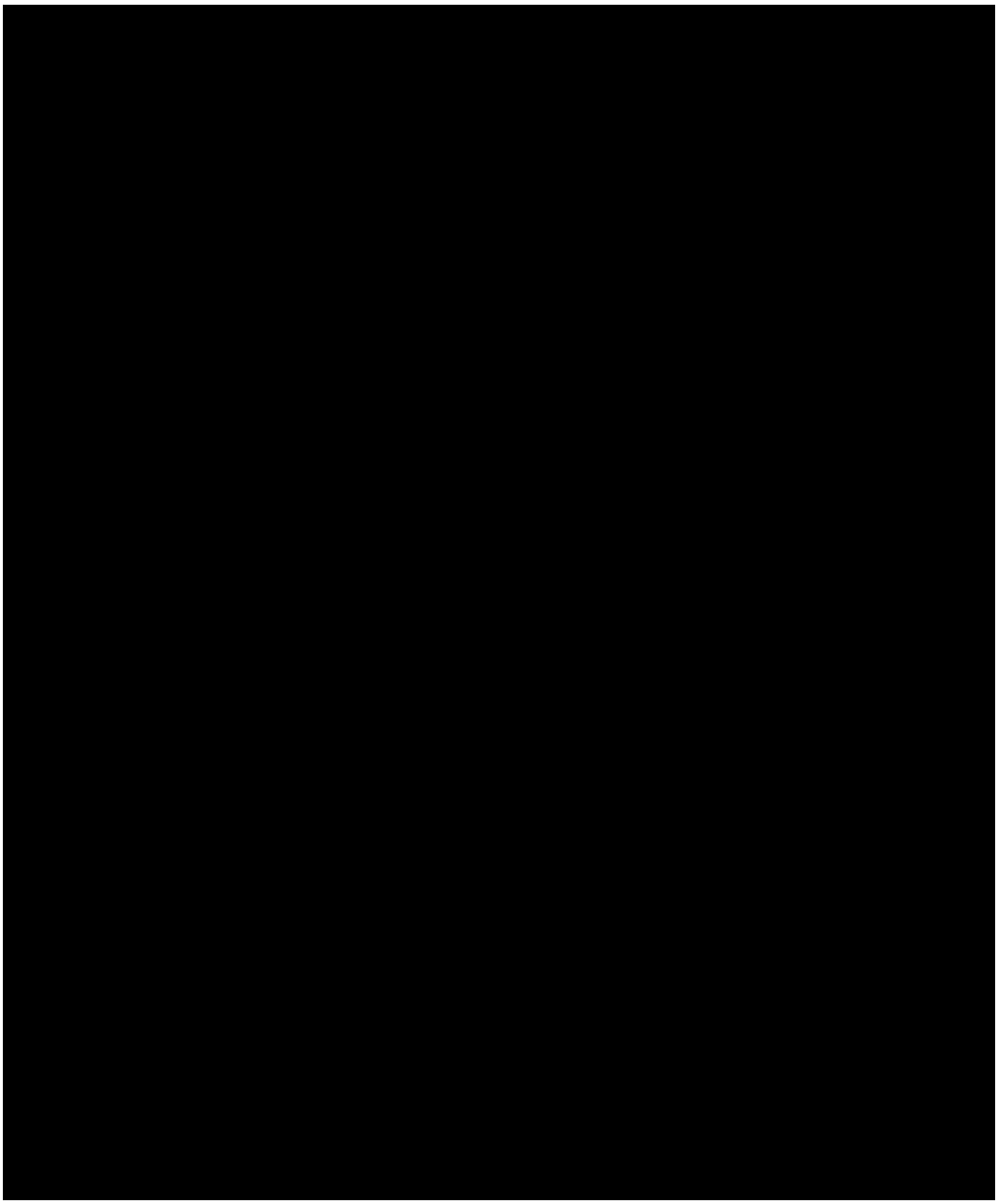

Figure 2-11 CALEA TCP/IP Access Via PSUEN XAT - BRI/XAT SVC: CDC Delivery

Figure 2-12 illustrates the generation of CDC messages in the SMP by the CALEA application. The messages are encapsulated by the Core PCP/IP software located in the SMP, relayed to the delivery PH for transmission to the appropriate PSUEN XAT PH channel group member and delivered over the SVC (X.25 network) to the X.75/X.75' interface where the Law Enforcement Agency (LEA) is served directly by the subject's switch. The PSUEN XAT and X.75/X.75' interfaces must reside on different PHs.

NOTE: The *5ESS*® switch serving the Remote LEA in Figure 2-12 (Switch II) is not required to be updated to the 5E16.2 Software Release.

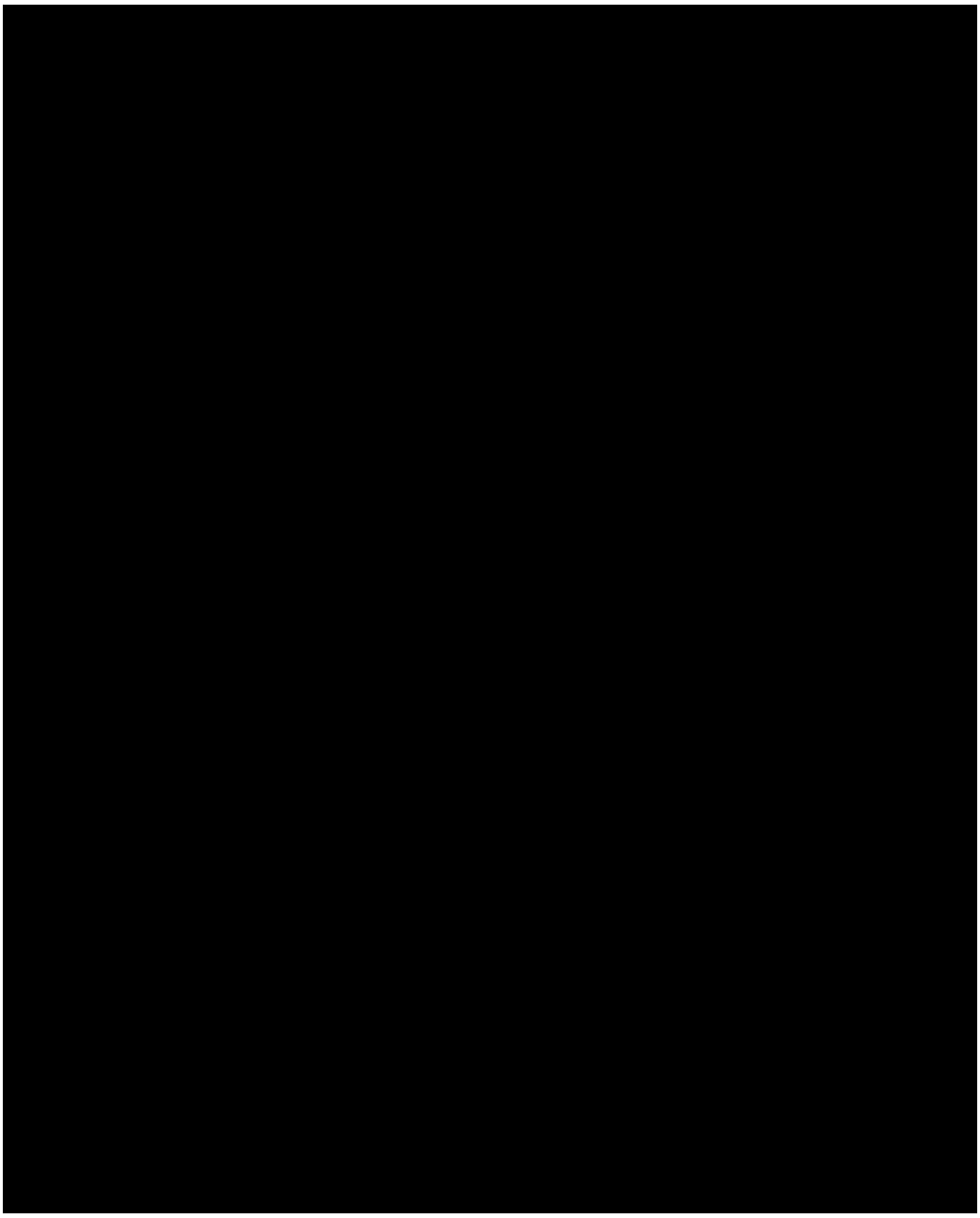

Figure 2-12 CALEA TCP/IP Access via PSUEN XAT - X.75/X.75' SVC: CDC Delivery

2.2.5 ICMP OVERVIEW

Internet Control Message Protocol (ICMP) is part of the transport layer, but, since ICMP is considered an extension of IP, it also maps to the layer containing IP. ICMP will respond to ECHO REQUEST ICMP messages (also known as "ping" messages) and will send an ICMP ECHO REQUEST message.

ICMP is covered in more detail in the IP LAYER chapter.

2.2.6 SIGNALING RATES

The dedicated BRI consists of two 64-kbps B-channels to support circuit-switched data (CSD) and packet-switched data (PSD) services. The dedicated XAT interface supports a provisionable signaling rate of either 56 kbps or 64 kbps.

2.2.7 GR-30 Overview

GR-30 based CDC transport is based on the caller-ID with call waiting service. Once the CDC link is provisioned, a pre-formatted CDC Connection Test Message requesting login may be automatically sent to the Law Enforcement Agency (LEA). The login message is sent by the 5ESS to the LEA to request the collection box (CB) to send the login ID to the switch.

The login ID is universal for all GR-30 links on the switch. When the CB sends the login ID, the 5ESS verifies it. The 5ESS maintains the CB's verification status - either unverified, correct login ID received, or incorrect login ID received. Regardless of verification status, the CB will still get CDC messages from the 5ESS.

Once set-up, the GR-30 CDC link will transmit the ASN.1 encoded CDC messages in Single Data Message Format (SDMF) packets using Frequency Shift Key (FSK) signaling at 1200 bits per second. Each CDC message is sent in one or more CDC packets. These packets are sent in order - the first is in a Begin packet, the last in an End Packet, and the remainder in Continue packets. All fragments of one CDC message will be sent before starting the next message.

All packets have a checksum, and if the CB determines the packet is bad, it can send the 5ESS a NACK to force retransmission of a bad CDC message. NACK'ing one packet forces resending of an entire CDC message.

If all packets are good, the CB then sends an ACK signal to the 5ESS for the entire packet and assembles the CDC message from the packets. If the link is inactive, another heart beat (specially formatted ConnectionTest CDC) message can be sent periodically from the 5ESS to the CB.

2.3 GRAPHICAL REPRESENTATIONS OF INTERFACES

NOTE: Some of the following graphics include the X.75/X.75' trunks only to show the capability of data transport over various data network layouts. **Only an X.25 BRI B-channel or XAT can be physically connected to the LEA collection facility.** X.75/X.75' trunks may be part of an overall data network, but are never directly connected to an LEA collection facility, therefore, X.75/X.75' trunks are outside the scope of this document.

Figure 2-13 displays the generation of CDC messages in the SMP by the CALEA application, which are encapsulated by the Core TCP/IP software located in the SMP, and relayed to the delivery PH for transmission to the appropriate X.25/XAT interface, where the Law Enforcement Agency is served directly by the subject's switch. Permanent Virtual Circuits are used in the X.25 network.

Figure 2-13 CALEA Core TCP/IP Access via X.25 BRI/XAT: CDC Delivery

Figure 2-14 displays the generation of CDC messages in the SMP by the CALEA application, which are encapsulated by the Core TCP/IP software located in the SMP, and relayed to the delivery PH for transmission to the appropriate X.75/X.75' interface where the Law Enforcement Agency is served outside of the subject's switch. Permanent Virtual Circuits are used in the X.75/X.75' network.

NOTE: The *5ESS*® switch serving the Remote LEA in Figure 2-14 (Switch II) is not required to be updated to the 5E14 software release.

Figure 2-14 CALEA Core TCP/IP Access via X.75/X.75': CDC Delivery

Figure 2-15 displays the 5E16.2 generation of CDC messages in the SMP by the CALEA application using GR-30 FSK signaling These GR-30 CDC messages are transmitted over an analog line termination to a Law Enforcement Agency which is served directly by the subject's switch.

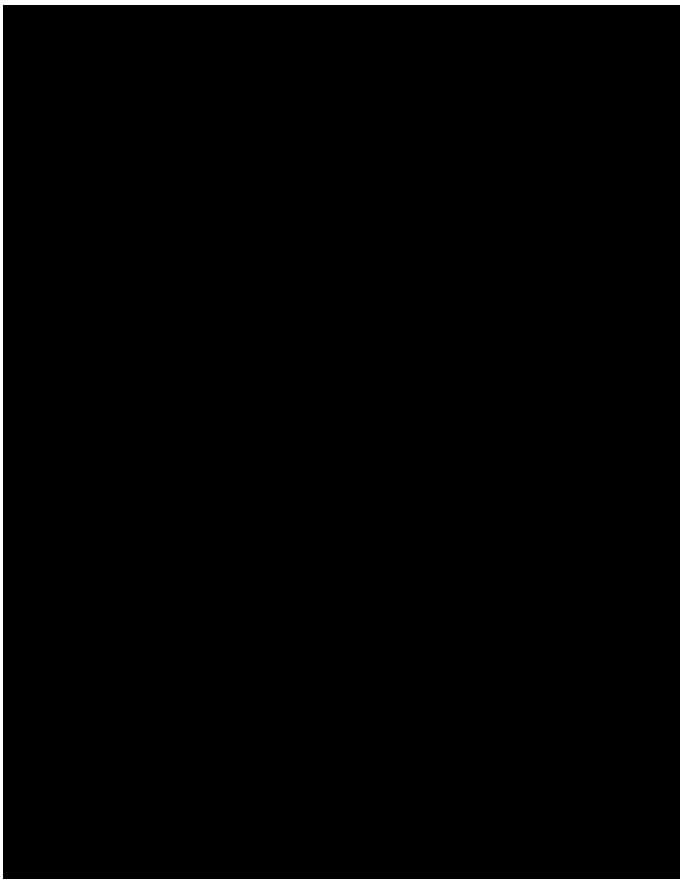

Figure 2-15 CALEA GR-30 Access via Analog Line: CDC Delivery

Figure 2-16 displays the 5E16.2 generation of CDC messages in the SMP by the CALEA application using GR-30 signaling. These GR-30 CDC messages are transmitted via trunks through the Public Switched Telephone Network to a Law Enforcement Agency which is not served directly by the subject's switch.

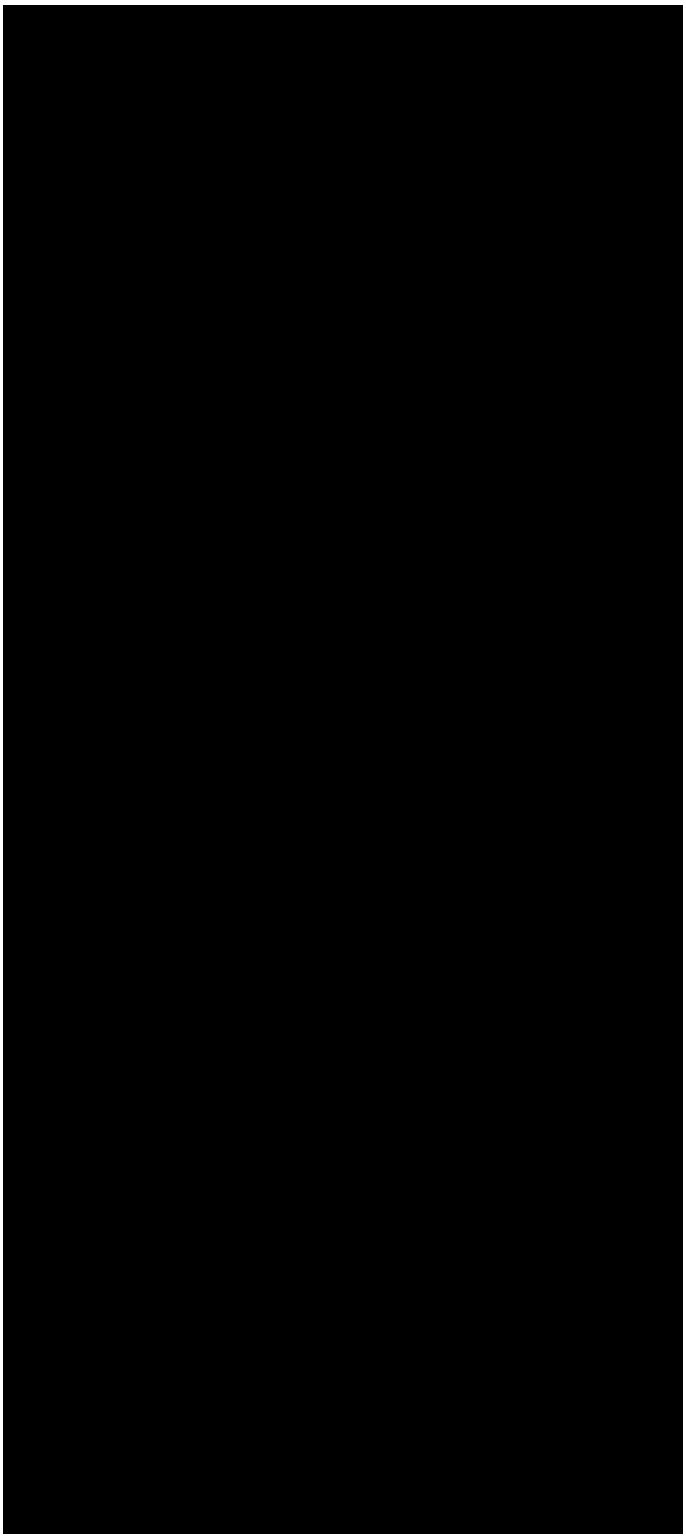

Figure 2-16 CALEA GR-30 Access via PSTN: CDC Delivery

Figure 2-17 displays the generation of PDC packets in the subject's PH for the CALEA application by copying all packets received and transmitted from the subject. These copied packets are then encapsulated by the Core TCP/IP software located in the subject's PH and relayed to the delivery PH for transmission to the appropriate X.25 or XAT interface, where the Law Enforcement Agency is served directly by the subject's switch. Here the subject's PH and the delivery PH are located in the same Packet Switching Unit (PSU). Permanent Virtual Circuits again are used in the X.25/XAT network.

Figure 2-17 CALEA Core TCP/IP Access via X.25/XAT: PDC Intra-PSU Delivery

Figure 2-18 displays the generation of PDC packets in the subject's PH for the CALEA application by copying all packets received and transmitted from the subject. These copied packets are encapsulated by the Core TCP/IP software located in the subject's PH and relayed to the delivery PH for transmission to the appropriate X.25 or XAT interface, where the Law Enforcement Agency is served directly by the subject's switch. Here the subject's PH and the delivery PH are located in different Switching Modules, so an Inter-SM PH with IP routing is required. Permanent Virtual Circuits again are used in the X.25/XAT network.

Figure 2-18 CALEA Core TCP/IP Access via X.25/XAT: PDC Inter-SM Delivery

Figure 2-19 displays the generation of PDC packets in the subject's PH for the CALEA application by copying all packets received and transmitted from the subject. These copied packets are encapsulated by the Core TCP/IP software located in the subject's PH and relayed to the delivery PH for transmission to the appropriate X.75 or X.75' interface, where the Law Enforcement Agency is served outside of the subject's switch. Here the subject's PH and the delivery PH are located in different Switching Modules, so an Inter-SM PH with IP routing is required. Permanent Virtual Circuits again are used in the X.75/X.75' network. Note, the *5ESS*® switch serving the Remote LEA in Figure 2-19 is not required to be updated to the 5E14 software release.

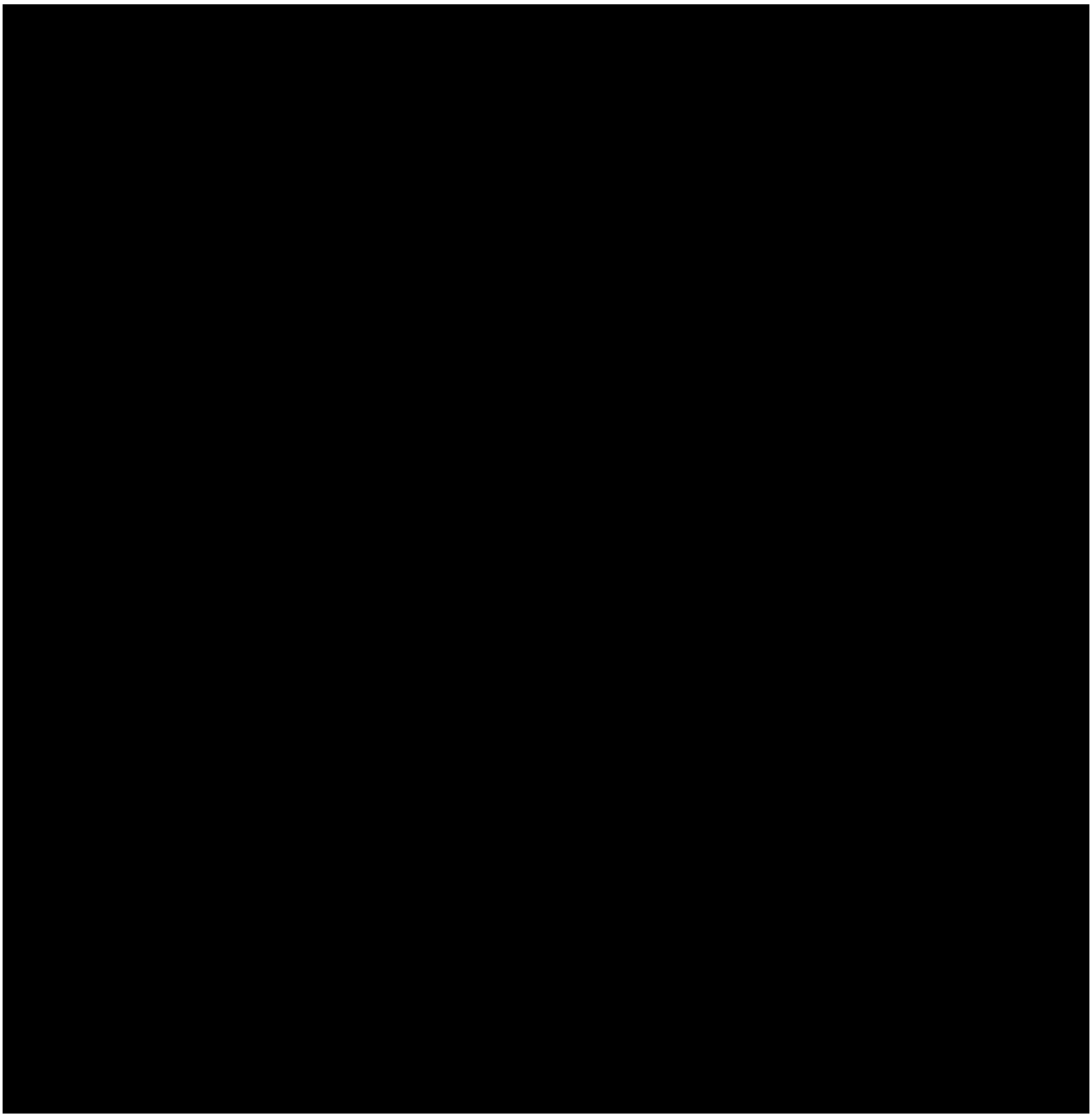

Figure 2-19 CALEA Core TCP/IP Access via X.75/X.75': PDC Inter-SM Delivery

The Call Content Channel (CCC) is a dedicated transmission path used to deliver circuit-switched voice and/or circuit-switched data call content from the switch to the LEA. The switch supports a separated CCC, meaning that the path is made up of a pair of trunks, one used to transport data sent by the subject and the other used to transport data sent to the subject. If the subject is under surveillance by multiple LEAs, then CCC fanout allows multiple CCCs to carry the call content to multiple LEAs. Figure 2-20 represents a subject being monitored by multiple LEAs. The subject may reside on an SM other than the delivery SM.

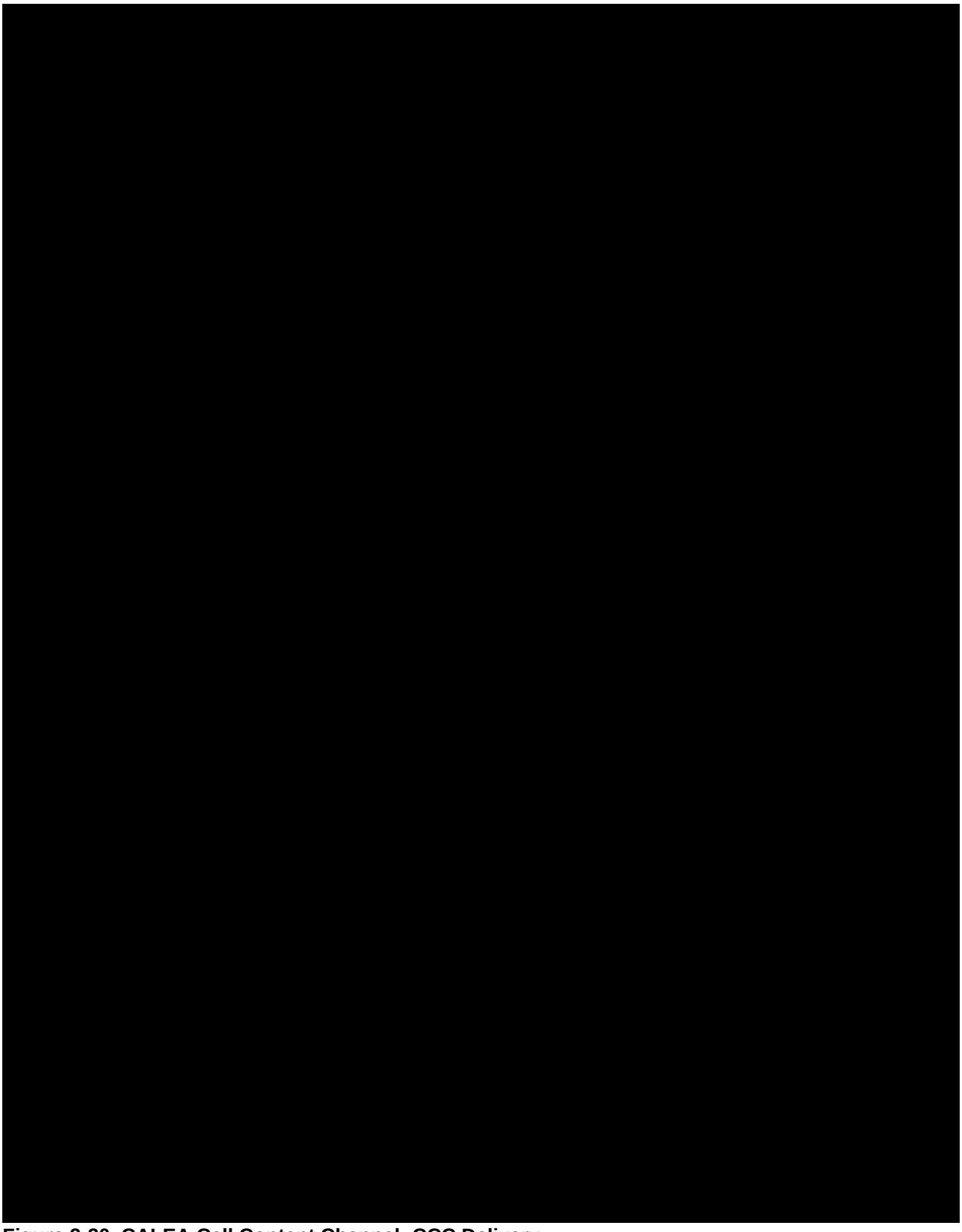

Figure 2-20 CALEA Call Content Channel: CCC Delivery

The dial out CCC separated option consists of a pair of trunks, one used to transport data sent by the subject and the other used to transport data sent to the subject. For CCC dial out, the CCC channel does not have to be connected to the CCC delivery SM. The trunks are routed through a PSTN to a single LEA. Figure 2-21 represents a separate mode configuration for a dial out CCC.

Figure 2-21 Dial Out CCC Delivery Separate Mode

The dial out CCC combined option consists of one CCC used to transport and send data for all call types. The trunk is routed through a PSTN to a single LEA. Figure 2-22 represents a combined mode configuration for a dial out CCC.

Figure 2-22 Dial Out CCC Delivery Combined Mode

2.4 TONE DECODERS (5E15 and later)

2.4.1 WHAT IS A TONE DECODER?

A tone decoder (also referred to as a universal tone decoder [UTD]) collects digits dialed by the subject. These digits are sent to the LEA if provisioned on the LAES case assignment view.

The tone decoder usage threshold for the office is specified on Recent Change view 8.1 (**TD LIMIT** field). The range of the parameter is 0% to 90% with a default value of 50%. This threshold is used to control when tone decoders are dropped from surveillances where no digits have been collected for more than 1 minute.

2.4.2 CALEA PUNCHLIST USAGE OF TONE DECODERS

The CALEA Punchlist feature provides dual tone multifrequency (DTMF) dialed digit extraction, which is required for both Level 1 and Level 2 subjects. Dialed digit extraction applies to the entire talk state of a call, not just address signaling. DTMF dialed digit extraction increases UTD usage.

The switch attempts to assign a universal tone decoder (UTD) to a Level 1 or 2 subject's call if all of the following are true:

(1) The call is originated by a subject with circuit-switched service.

NOTE: Calls terminating to a subject are not assigned a UTD for CALEA.

NOTE: Packet calls are not assigned a UTD for CALEA.

(2) The subject profile (view C.4) has field "DTMF STATUS" set to ESSENTIAL or STANDARD.

NOTE: The possible values for DTMF STATUS are:

ESSENTIAL	= Tone decoder will not be dropped during the call.
STANDARD	= Tone decoder will be dropped if a threshold tone decoder usage is reached.
NONE	= no tone decoder is attached to this subject's calls (DTMF is disabled)

(3) Level 1 subjects only - The call is dialed with a Carrier Interconnect type (CITYPE) that has DTMF extraction enabled.

NOTE: The CITYPE assignment per call is done in switch digit analysis translations, for example, view 9.3.

NOTE: The CITYPEs that will receive DTMF extraction are selected by the Surveillance Administrator on RC view C.1.

(4) The call is routed with a Bearer Capability that is not "Circuit Switched Data."

(5) An Idle UTD circuit is available at the time of call setup.

The collection of subject-dialed digits buffers the lesser of 32 digits or 20 seconds of delay. The switch sends a DialedDigitExtraction message to the LEA when either 32 digits are collected or when 20 seconds has passed since the last digit collection message.

At the end of the call, any remaining digits (not previously sent) are sent to the LEA in a DialedDigitExtraction message that precedes the CDC Release message. If the subject does not enter any post cut-through DTMF digits, then no DialedDigitExtraction message is sent.

If no tone decoder is available for a call under surveillance with a LAES case marked as "ESSENTIAL" or "STANDARD", then a DialedDigitExtraction message is sent to the LEA collection facility indicating "No Tone Decoder Available" in the "Digits" field.

2.4.3 DROPPED TONE DECODERS

Tone decoders may be dropped for one of several reasons. When a tone decoder is dropped or cannot be applied to a call, the switch sends an alarm message (REPT CALEA SAS) to the Surveillance Administration System terminal and the LEA collection facility.

The reasons for not applying or removing a tone decoder from a surveillance are:

(1) The switch received a burst of digits greater than 100 digits in 20 seconds.

NOTE: The digits per second threshold may **not** be changed by the switch owner (service provider).

(2) The CALEA tone decoder threshold was exceeded.

(3) The tone decoder was dropped due to other failure/maintenance.

(4) No tone decoder was available.

2.4.3.1 CALEA UTD Load Shedding

For every "active call" surveillance, the level of available tone decoders is checked every 20 seconds. The TD LIMIT field in Recent Change view 8.1 is used to specify the percentage of available tone decoders to be used at any one time.

The TD LIMIT office parameter applies to all SMs in an office, however, the switch monitors tone decoder usage on a per SM basis. DTMF dialed-digit extraction load-shedding is performed when all of the following conditions are met:

(1) When the total number of tone decoders currently in use for the subject's SM exceeds the percentage of equipped tone decoders (specified in the TD LIMIT field on view 8.1).

(2) The subject's case is has DTMF STATUS marked "Standard".

(3) The subject has not dialed any digits for one minute.

If these conditions are met, then the UTD is released from the subject's call, and a DialedDigitExtraction message is sent to both the Surveillance Administration System terminal and the LEA collection facility indicating "Tone Decoder Dropped Due To Load" in the "Digits" field.

Once a tone decoder is dropped, no further dialed digits may be collected for the subject's call.

2.4.3.2 Surge of Digits

The tone decoder will be dropped due to a surge of digits, even if the collection of post cut-through digits (DTMF STATUS field) is marked "ESSENTIAL" in the LAES case (view C.4). This action protects the switch resources from a possible hardware failure. When a surge of digits causes a tone decoder to be dropped, a DialedDigitExtraction message is sent to both the Surveillance Administration System terminal and the LEA collection facility indicating "Digit Surge Tone Decoder Dropped" in the "Digits" field.

3. PHYSICAL, LINK, AND NETWORK LAYERS

3.1 OVERVIEW

The ITU-T recommendations on ISDN access protocols reflect the multilayer Open Systems Interconnection (OSI) reference model. Specifically, ITU-T standards cover the OSI model's first three service layers: layer 1 (the physical layer), layer 2 (the data-link layer), and layer 3 (the network layer).

Two user-network interfaces, the "National interface" and the "Custom interface" are supported in the 5E14 software release. The Bellcore-defined National ISDN protocols and services on the Standard interface are documented in the 235-900-341, *5ESS® Switch National ISDN BRI Specification*.

The Custom interface which also supports the Lucent ISDN protocols and services are documented in the 235-900-343, *5ESS® Switch Custom ISDN BRI Specification*.

NOTE: This Chapter contains CALEA-specific information. For all other specifications relating to these three layers, please refer to the BRI Specification documents.

3.2 PHYSICAL LAYER

3.2.1 ISDN SUBSCRIBER LINE INTERFACES - GENERAL

The ITU-T recommendations on ISDN access protocols reflect the multilayer Open Systems Interconnection (OSI) reference model. Specifically, ITU-T standards cover the OSI model's first three service layers: Layer 1 (the physical layer), Layer 2 (the data-link layer), and Layer 3 (the network layer).

Two user-network interfaces, the "Standard interface" and the "Custom interface" are supported. The Bellcore defined National ISDN protocols and services on the Standard interface are documented in the 235-900-341, *5ESS® Switch National ISDN BRI Specification*. In addition to the Standard interface, the Custom interface will also support the Lucent ISDN protocols and services. For complete information on the Custom interface, refer to the 235-900-343, *5ESS® Switch Custom ISDN BRI Specification*.

3.2.2 ISDN SUBSCRIBER LINE INTERFACES - PHYSICAL LAYER

The physical layer encompasses the movement of bits over physical media and requires physical-interface and electrical-interface specifications such as bit formats, timing, and voltage levels. The *5ESS®* switch supports two Layer 1 interfaces: the T-interface and the *ANSI®* 2B1Q U-interface. The Custom and Standard interfaces support both Layer 1 interfaces.

NOTE: An NT1 device will be required if the terminating CPE is a 4-wire T-interface. The NT1 converts the 2-wire U-interface signal to the 4-wire T-interface signal. The NT1 supports point-to-point and multipoint ISDN services. The NT1 must be in the same building as the terminal. That is, no outside plant wiring between NT1 and ISDN terminal equipment.

The implementation of ISDN requires the service provider to be sensitive to loop loss. Refer to 533-700-100, *Customer Premises Planning Guide*, when calculating loop loss. Loop qualifications must be made for the T-interfaces.

According to the *ANSI®* standards, attenuation of the T-interface cable plant should be limited to 6 dB measured at 96 kHz; therefore, the T-interface is typically used for intra-building applications. The maximum distance for the T-interface is approximately 1,900 feet for typical customer premises inside wiring (24-gauge DIW).

It is recommended that individual loops need not be qualified to support the *ANSI®* U-interface since 98 percent of all nonloaded subscriber loops will operate satisfactorily. Loop loss should not exceed 33.4 dB measured at 20 kHz. When 2B1Q is deployed, the maximum distance increases to approximately 18,000

feet.

3.2.2.1 T-INTERFACE

The T-interface was recommended by the ITU-T in 1984. It is consistent with ITU-T Recommendation I.430 and with *ANSI*® Standard T1.605-1989. The T-interface supports both Custom and Standard interfaces.

The T-interface provides a 4-wire, balanced transmission interface. One wire pair is used to transmit and the other wire pair is used to receive. The signaling rate for the T-interface is 192 kbps, consisting of two 64-kbps B-Channels, one 16-kbps D-Channel, and 48 kbps of overhead information. Data is grouped in 48-bit frames in both transmission directions. 48 bits are transmitted in 250 microseconds; 4,000 frames are transmitted in a second.

The T-interface can originate either at the T-line card residing at the *5ESS*® switch or at an NT1 at the customer premises.

3.2.2.2 *ANSI*® U-INTERFACE

The *5ESS*® switch *ANSI*® U-interface is consistent with the *ANSI*® T1.601-1988 Standard. The *ANSI*® U-interface supports both Custom and Standard interfaces.

This transmission system uses the echo canceler with hybrid principle to provide full duplex operation over a 2-wire subscriber loop. With this system, the echo canceler produces a replica of the echo of the near-end transmission, which is then subtracted from the total received signal.

Transmission rates of up to 160 kbps are supported by the U-interface. The 2B1Q (2 binary, 1 quaternary) data encoding method causes data to appear in an 80-kbaud format. 2B1Q means that two binary bits of data are transmitted in one time slot as one of four signal levels.

The loop frame is 240 bits long, yielding a frame duration of 1.5 ms. The first 18 bits generate the synch-word pattern providing frame and superframe delineation. The next 216 bits represent 12 blocks of 2B+D information, of 18 bits each. The remaining six bits provide overhead or maintenance functions.

A 12-ms superframe is constructed from 8 loop frames. The superframe structure start is marked by an inversion of the synch-word framing pattern in the first frame of the superframe. The specific functions attributed to the overhead bits correspond to their respective positions in the superframe.

The establishment of framing and superframing over the loop and synchronization of framing and superframing between the line and network termination is autonomously established by the transceiver hardware.

3.2.3 CALEA DELIVERY CHANNELS

3.2.3.1 CCC: Call Content Channel

Circuit-switched voice (CSV) and circuit-switched data (CSD) call content is copied from the switching matrix, encoded using standard network bearer services, and transported to the LEA via a CCC pair. The intercepted content is delivered without modifying the content within the quality objectives for the intercepted network bearer service. Speech and 3.1 kHz audio bearer services intercepted and delivered over circuit-mode digital facilities use the □-law encoding of ITU-T Recommendation G.711, "Pulse Code Modulation (PCM) of Voice Frequencies."

To maintain data integrity, CCC trunks always apply OdB loss.

Each time a call content channel is assigned to deliver call content, a message indicating channel identities for the transmit and receive call content is sent over the call data channel (CDC) to law enforcement.

NOTE 1: If a subject has call redirection features and/or conference call and multi-party hold features, more than one CCC pair may be ordered by the LEA.

NOTE 2: CCCs are a component of the Physical Layer only. CCC is nothing more than DS0 on a T1; therefore, it is not impacted by higher layers of protocol.

NOTE 3: 0db loss applies to dial out CCCs as well. For 5E16.2 software release only one Level 2 surveillance case is supported per subject if the CCC dial out option is used.

3.2.3.1.1 Dedicated Call Content (CCC)

For a given surveillance, call content will be delivered over a dedicated CCC pair (one CCC for subject side and the other for non-subject side call content). Dedicated channels are permanent connections that do not pass through any type of switching matrix. These are sometimes called nailed-up circuits. When the IAP switch needs to deliver circuit-switched call content, it replicates the content from the switching matrix and places a copy onto the appropriate dedicated channel. The *5ESS*® switch supports the separated CCC option, where separate channels are used for transmit and receive circuit-switched call content. CCCs are assigned to a subject or associate surveillance one by one because various call scenarios can add one CCC for each associate connected to the call.

Each CCC dedicated trunk circuit has only one intercept subject assigned to it. Additional dedicated trunk circuits are required for each subject and LEA. All trunk circuits within a CCC trunk group will terminate to the same LEA collection facility. Within a trunk group, trunk member numbers for a single subject must be contiguous.

NOTE: CCCs should be assigned to a surveillance in the same pairing (fixed association) so that the LEA will know which two trunk members will be associated with a given surveillance. The Surveillance Administrator inputs the first member number of the CCC pair. The switch software automatically assigns the next member number to complete the pair.

CCC trunks must be digital trunks providing time multiplexed signals (T1) complying with digital formats given in *ANSI*® T1.107-1988. The electrical interface for digital CCCs must comply with *ANSI*® T1.102-1987. The main points to remember regarding CCC trunks are:

- 0dB loss is applied.
- The trunks have 0-state signalling.
- C-Tone is provisioned in the office.

3.2.3.1.2 Dial Out Call Content Channel (CCC)

The Dial Out Call Content Channel (CCC) feature (99-5E-8221) is available in Software Release 5E16.2 and later.

When a subject is provisioned for surveillance using dial out CCC, a LEA local DN and a LEA destination DN will also be provisioned.

NOTE: Only one LEA destination DN per subject is allowed and it may be either local or remote to the switch. Refer to Figures 3-1 and 3-2 for a block diagram of each possible dial out CCC network configuration. The LEA local DN is used to forward the CCC to a real destination, which is the DN of the LEA collection box. The LEA local DN exists only in data and is not a physical telephone or terminal. The Local LEA DN must be assigned to a physical LU similar to what is required for lines with Remote Call Forwarding. In addition, it will be provisioned with an active call forwarding variable feature, however the forward-to DN will be ignored when calls are terminated to it. Calls to the LEA local DN will be forwarded to the DN of the the LEA collection box which is referred to as the LEA destination DN. The switch will provide a CCC ID to associate a call with a specific

surveillance. The CCC ID will be generated by the switch, and will be a random number that is six digits in length with a 0, 1 or 2 prepended. The 0, 1 or 2 represents transmit, receive or combined, respectively.

Surveillances performed with the dial out CCC feature can select between three different call content delivery modes:

- **Separated Mode:** Two dial out call content channels are set up: one for the transmit and one for the receive path. Both transmit and receive CCC will be routed with the same DN and then forwarded to the LEA destination DN.
- **Combined Mode:** Only one call content channel is allocated to carry both transmit and receive call content for all call types.
- **Mixed Mode:** If the Bearer Capability (BC) of the monitored call is "speech" or "3.1 audio", the combined mode is used. For any other BC types, separate mode is used.

The forwarding call's AMA is based on the destination DN (similar to the local LEA originating the call to the destination LEA).

The following is a high level scenario of dial out CCC being used to set up and perform the monitoring of an intercept subject. Before a CALEA surveillance case is provisioned for dial out CCC surveillance, the following information must be known:

- LEA local DN
- LEA Destination DN
- CCC delivery mode
- CCC identifier
  - CCC Identifier sent (pre stamp and/or post stamp via in-band tones)
- Add new CCC "answer timeout" timer

Once the aforementioned information is known, the surveillance administrator can use recent change to provision the case. The LEA local DN with call forwarding is provisioned on the switch that hosts the subject's line. In addition, the LEA destination DN, CCC delivery mode, the CCC identifier and whether it will be sent pre-stamp or post-stamp is provisioned on the switch.

When the subject initiates a call and dials one digit (assuming the surveillance option is set to "start after 1-digit"), the switch performs a CCC dial out by initiating a call to the LEA local DN. If the surveillance option is set to "start after routing", the switch will wait until the subject has completed dialing and routing has started before initiating a call to the LEA local DN. The CCC call is then forwarded to the LEA destination DN. With combined and circuit-switched voice (CSV) mixed modes, a 3-way conference circuit is allocated by the switch for the surveillance. While waiting for an answer from the dial out CCC, the switch will bridge onto the subject line. After successful bridging and answer supervision from the destination LEA, a CCOpen CDC message with the correct CCC identifier is sent to the LEA via CDC.

After the intercepted call is ended, the switch will send the CCC identifier with in-band tones to the LEA via the CCC channel if post-stamp option is set. Once the in-band tones are sent, the CCC will be torn down and a CCClose CDC message with the same CCC identifier will be sent to the LEA via CDC. If only pre-stamp option is set, no in-band tones will be sent. The CCC will be torn down and a CCClose CDC message will be sent right after the intercepted call is ended.

NOTE: C-tone does apply to the dial out CCC feature. If the service provider or the LEA desires to test the correctness of the CCC dial out provisioning, then the verify office command can be used to simulate a call from the subject DN. Another option would be for the service provider to use one of the office test lines as a subject line and test the CCC dial out capability by making calls from and to the test line.

Figure 3-1 shows a possible dial out CCC network configuration with a local LEA Destination DN provisioned.

Figure 3-1 CCC Dial Out with Local LEA Destination DN

Figure 3-2 shows a possible dial out CCC network configuration with a remote LEA Destination DN provisioned through a public switched telephone network.

Figure 3-2 CCC Dial Out with Remote LEA Destination DN

3.2.3.2 PDC: Packet Data Channel

Packet call content data is conveyed to the LEA monitoring station (MS) using a pair of TCP socket connections called the packet data channel (PDC). One socket connection is used to transport data sent by

the subject and the other socket connection is used to transport data sent to the subject. Each PDC TCP connection is supported by a X.25 permanent virtual circuit (PVC) to transport packet call content from the *5ESS*® switch to the LEA monitoring station. Therefore, the physical media can be either a BRI or T1 (XAT).

3.2.3.3 CDC: Call Data Channel

Each SMP TCP connection is supported by an X.25 permanent virtual circuit (PVC) to transport CDC messages from the switch to the LEA monitoring station. Therefore, the physical media can be either a BRI or a T1 (XAT).

With the CDC dial out option, Switched Virtual Circuits (SVC) sockets are established from an XAT PH Channel Group Member emulating an X.25 DTE to a local LEA facility via a BRI or XAT termination. The SVC can also be established from the emulating X.25 DTE to a remote LEA via a X.75 or X.75' packet network.

The CDC Using Voiceband Data Transmission feature (99-5E-8318) allows CDC messages to be transmitted using an analog line interface. The CDC messages can be routed to a local LEA or to a remote LEA over a trunk via the public switched telephone network.

3.3 X.25 LINK LAYER

3.3.1 OVERVIEW

Layer 2, the link layer, defines the frame structure, elements of procedure, format of fields, and procedures for the proper operation of the Link Access Procedure Balanced (LAPB).

For CALEA, X.25 service is provided to ISDN subscribers via permanent packet B-Channel (PPB) packet switching. PPB uses the Link Access Procedure Balanced (LAPB) as the Layer 2 protocol as specified in the 1984 Recommendation for X.25. The procedures for X.25 virtual circuit service are in conformance with the 1984 ITU-T X.25 Recommendation procedures. PPB requires that a nailed-up access connection be established between a basic rate interface (BRI), the packet switch unit (PSU), and an integrated services digital network switching module (ISDN SM). This is accomplished via a nailed up Layer 1 interface between the BRI U-interface or T-interface line card and the packet handler (PH) in the PSU.

For 5E16.2 software release, X.25 SVC connection is established from a PSUEN XAT (no layer 1 or layer 2) on a PSU PH (packet switch unit protocol handler) channel group member using a specified LCN (logical channel number). Multiple surveillance cases may use the same X.25 SVC LCN as long as the same X.25 destination is used. Parameter k (window size) is restricted to seven and receives/transmits packet size is restricted to 128 for PSUEN XAT interface.

3.3.2 DATA LINK LAYER SPECIFICATIONS FOR THE B-CHANNEL

The Link Access Procedure Balanced (LAPB) specified in ITU-T Recommendation X.25 (1984 X.25, Section 2) is used in the case of B-channel packet transport mode service. This section addresses only unspecified areas of LAPB, or those for which implementation option specifications are required.

The *5ESS*® switch supports the LAPB single link procedures, but not the LAPB multilink procedures specified in Section 2.5 of ITU-T Recommendation X.25.

The LAPB frames supported by the *5ESS*® switch must always consist of an integral number of octets.

The B-channel links come into existence at the *5ESS*® switch in a disconnected phase. The switch initiates link setup under only one of the following conditions:

- when a new B-channel is provisioned

- when a B-channel is restored
- when a network is initialized.

If the reset fails, the *5ESS*® switch will enter the disconnected phase and wait for the user to initiate link reset. The switch responds to the receipt of a set asynchronous balanced mode (SABM) command from the user side as specified in Section 2.4.4.1 of ITU-T Recommendation X.25.

The switch supports only the basic mode (modulo 8) of LAPB, as specified in Section 2.4.1 of ITU-T Recommendation X.25.

3.3.2.1 LAPB SYSTEM PARAMETERS

Section 2.4.8 of ITU-T Recommendation X.25 defines several system parameters without specifying their values. The following values are required for the implementation of packet transport mode service.

- T1 Timer (retransmission delay timer) is set per link, by service order, within a range of 0.4 through 20 seconds (default = 1 second), in approximately 0.2-second increments.
- T3 Timer (idle timer determining how often polling occurs on an idle layer 2 link) is set per link, by service order, within a range of 1 through 26 seconds (default = 3 seconds) in 2-seconds increments, and must be at least as large as T1.
- Parameter N1 (maximum number of octets included in the I frame) has a fixed value of 2112 bits, supporting a maximum I-field size of 264 octets; the information field is restricted to an integral number of octets.
- Parameter N2 (maximum number of frame retransmissions following an expired T1 timer) is set per link, by service order, within a range of 1 through 15 (default = 2), in unitary increments.
- Parameter k (window size, or the number of unacknowledged transmissions allowed to be outstanding) is set per link, by service order, within a range of 2 through 7 (default = 7), in unitary increments.

The X.25 specification states that the network side parameters T1, T2, T3, N1, and N2 "shall be made known" to the user side, and that the user side parameters T1, T2, N1, and N2 "shall be made known" to the network side. X.25 suggests no actual mechanism for making the information known. The *5ESS*® switch requires external administrative procedures for this purpose. The network-side values are negotiated with the user-side administrator through the service provider's service ordering process; similarly, any needed information concerning the user-side parameters is passed to the switch by the service provider through standard recent change procedures.

3.3.2.2 LINK SETUP PROCEDURE FAILURE HANDLING

Section 2.4.4.1 of ITU-T Recommendation X.25 states that after N2 occurrences of the network sending an SABM frame to request link setup, followed by a failure of the user side to respond with a unnumbered acknowledgment (UA) or disconnected mode (DM) frame within T1 seconds, the network side initiates "appropriate higher level recovery action." The appropriate action is unspecified. The *5ESS*® switch responds to this failure by entering the disconnected phase defined in "Data Link Layer Specifications for the B-Channel," Section 3.3.2 .

3.3.2.3 EXPIRATION OF TIMER T3

Timer T3 detects an excessively long idle channel state condition on the link level. At the expiration of Timer T3, the *5ESS*® switch will follow the link disconnection procedure as described in Section 2.4.4.3 of ITU-T Recommendation X.25.

3.3.2.4 LINK DISCONNECTION PROCEDURE FAILURE HANDLING

Section 2.4.4.3 of ITU-T Recommendation X.25 states that after N2 occurrences of the network side sending a DISC frame to request link disconnection, followed by a failure of the user side to respond with a UA or DM frame within T1 seconds, the network side initiates "appropriate higher level recovery action." Again, the appropriate action is unspecified within ITU-T Recommendation X.25. The *5ESS*® switch responds to this failure by entering the disconnected phase defined in "Data Link Layer Specifications for the B-Channel," Section 3.3.2 .

3.3.2.5 RNR AND TIMER RECOVERY PROCEDURE FAILURES

Sections 2.4.5.7 and 2.4.5.9 of ITU-T Recommendation X.25 give the network side two options for responding to the occurrence of N2 timeouts in attempting to perform receiver-not-ready (RNR) and timer recovery procedures. The *5ESS*® switch responds to these failures by entering the disconnected phase described in "Data Link Layer Specifications for the B-Channel," Section 3.3.2 .

3.3.2.6 LINK RESET PROCEDURE FAILURE HANDLING

Section 2.4.7.2 of ITU-T Recommendation X.25 states that after N2 occurrences of the network side sending an SABM frame to request link reset, followed by a failure of the user side to respond with a UA or DM frame within T1 seconds, the network side initiates the "appropriate higher level recovery action." The *5ESS*® switch responds to this failure by entering the disconnected phase defined in "Data Link Layer Specifications for the B-Channel," Section 3.3.2 .

3.3.2.7 EXCESSIVE ERROR COUNT

If the *5ESS*® switch receives an excessive number of unexpected frames, which might indicate a malfunction at the CPE, the switch will deactivate the B-channel for a period of 5 minutes. At the end of the 5-minute period, the switch will reactivate the B-channel and attempt link setup.

3.4 X.25 NETWORK LAYER

3.4.1 OVERVIEW

The X.25 network layer protocol provides the means to establish, maintain, and terminate network connections across an ISDN between communicating application entities using a series of specific messages that move to and from the customer's terminal and the ISDN exchange.

The protocol supported herein conforms to the Recommendation X.25 (1984) Layer 3 specification for connecting packet mode data terminal equipment (DTE) to a packet handling function: setup, maintain the data transfer, and maintain the PVCs.

In addition, the network supports the following capabilities:

- A local interface between the network and a DTE conforming to the Recommendation X.25 (1980).
- Interworking between 1980 and 1984 X.25-based DTEs for ITU-T-defined end-to-end signaling.

For 5E16.2 software release, SVC initialization occurs when the first CDC message for a subject is ready to be sent to the LEA monitoring station. The CDC message or messages are buffered or queued until the X.25 SVC packet call is established from the specified LCN on a PSUEN XAT interface, to the destination X.25 packet address, IP connectivity and a socket has been established.

Similar to PVCs, SVCs must be in the range of 1 to 127. Minimal flow control is supported on the SVCs on a per-all basis, only a packet size of 128 and a window size of seven is supported.

3.4.1.1 BRI X.25 PVC

This section describes the X.25 procedures for the establishment and maintenance of permanent virtual circuits (PVCs) carried over a packet transport mode access connection. These procedures are defined in terms of X.25 packets exchanged over the packet mode access connection on the basic access interface structure. The functions and procedures of the protocol, and the relationship with other layers, are described in the 1984 ITU-T X-series Recommendations.

TCP messages may be routed from a PH to a dedicated BRI X.25 Permanent Virtual Circuit (PVC) as defined by provisioning. The X.25 PVC interfaces with the internal packet handler (PH) (supported on PH3 and PH4) for the data required for operation and control. PVCs are supported on permanent B-channel connections only. CDC messages and PDC packets are routed between the SMP or PH served by a subject and the dedicated BRI X.25 PVC to the Law Enforcement Agency monitoring stations. The IP address will map to a specific BRI and B-channel, and a specific PVC on that channel.

3.4.1.1.1 PVC INITIALIZATION

The CPE will receive a Reset Indication packet with cause "network operational" when the setup is complete (this does not necessarily mean that the PVC has been established). After the initialization of Layer 3, the following procedures apply:

- If the CPE attempts to send data or a reset request before the PVC has been established through the network, the network either will not respond or will send a Reset Indication packet with cause "out-of-order" on that PVC.

- If the CPE does not attempt to send data or a reset request until after the PVC has been established through the network, the CPE will be informed through a Reset Indication packet with cause "network operational," and the data or reset packet will undergo the normal data transfer procedures.

3.4.1.1.2 LOGICAL CHANNEL

Each X.25 logical channel is identified by a 4-bit logical channel group number and an 8-bit logical channel number. These channel numbers must appear in every X.25 packet except RESTART and DIAGNOSTIC.

Logical Channel 0 is reserved for control packets (RESTART and DIAGNOSTIC). As a subscriber option, 1 to 127 logical channels are supported for permanent virtual circuits on a communication link carried by a B-channel.

Logical channel assignment is in accordance with X.25, Annex A. Logical channel numbers assigned for PVCs must be in the range of 1 to 127 on the communication link carried by a B-channel. The range of logical channels for PVCs is specified by service provisioning. This range includes the assigned PVC, as well as logical channels for future PVCs. The user must specify the logical channel number of each active PVC at subscription time.

3.4.1.1.3 DATA/INTERRUPT TRANSFER

The procedures for data and interrupt transfer follow the procedures described in ITU-T Recommendation X.25, Section 4.3. For data transfer, the network delivers data packets to the terminating user side in the sequence in which the packets were transmitted by the originating user side; the network attempts to deliver the packets without packet duplication.

NOTE: The delivery confirmation bit (D-bit), qualifier bit (Q-bit), and more data mark bit (M-bit) are NOT supported. If the switch receives a packet with any of these bits set to "1", the switch sends a "Reset Indication" packet to the sender according to X.25.

NOTE: The Interrupt Packet is NOT supported. If the switch receives an Interrupt Packet, the switch sends

a "Reset Indication" packet to the sender according to X.25.

3.4.1.1.4 FLOW CONTROL

The network side follows the standard flow control principles specified in Section 4.4.1.3 of ITU-T Recommendation X.25. If the network side receives a data packet containing a packet send sequence number, P(S), that is out of sequence within the window, the network side resets the virtual circuit. The network side does not pass these packets across the network to the terminating user side equipment.

The network side uses service provisioning to allow negotiation on a per-call basis of the following flow control parameters:

(a) ***Packet Size:*** The network supports a maximum size of 256 octets of user data. The default size is 128 octets of user data.

(b) ***Window Size:*** The network supports window sizes of 1 to 7. The network defines a window for each direction of data transmission and for each end of a logical channel for a virtual call or PVC. A default window size of 2 is associated with the virtual call if neither side requests a window size value.

3.4.1.1.5 DIAGNOSTIC PACKET

The network side supports the use of DIAGNOSTIC packets to indicate error conditions under circumstances when the usual methods of indication (for example, reset, clear, and restart with cause and diagnostic codes) are inappropriate. The conditions under which the network side sends the DIAGNOSTIC packet are as specified in X.25, Section 3.4.1.

3.4.1.1.6 EFFECTS OF THE PHYSICAL LEVEL AND THE LINK LEVEL FAILURE

When the network side detects a failure on the physical level, the network side transmits toward the far-end user a reset for each PVC.

For a link failure (Layer 2, see "X.25 Link Layer," Section 3.3) the network handles all the virtual calls as a physical level failure.

3.4.1.2 XAT PVC

Routing of TCP messages is also supported from a PH (PH 3 or PH4) to a dedicated X.25 Packet Switching on T1 Facility (XAT) PVC as defined by provisioning. CDC messages and PDC packets are routed between the SMP or PH served by a subject and the dedicated XAT PVC to the Law Enforcement Agency monitoring stations. The IP address will map to a specific XAT and B-channel, and a specific PVC on that channel.

X.25 Packet-Switching Access on T1 Facilities (XAT) allows the use of X.25 packet-switched services on a preselected number of provisioned DS0 time slots. On a per-channel basis, each channel is connected by subscription to the packet handling function. At subscription, any number of channels may be requested on the T1.

NOTE: The DS0 time slot equates to one 64 or 56 kbps channel of a T1 line.

The subscribed packet-switched connection supports permanent virtual circuit services. No circuit-switched services are allowed on the channel selected for packet services. The 64 kbps channels on the T1 remain distinct (no aggregation for higher communication rate).

4. IP LAYER

4.1 OVERVIEW

The Internet Protocol (IP) layer is made up of IP and internet control message protocol (ICMP). IP provides for transmitting datagrams from a source to a destination, each identified by a unique, fixed-length address. IP also provides for fragmentation and reassembly of long datagrams. ICMP provides for error reporting in the processing of datagrams. For example, ICMP messages are sent when a datagram cannot reach its destination and when the gateway does not have the buffering capacity to forward a datagram. For fragmented datagrams, ICMP messages are sent only about errors in handling fragment zero.

4.2 INTERNET PROTOCOL

An end host attaches the IP address and forwards the packet to a router. The router consults the IP address, refers to a table of IP addresses, and forwards the packet. The next router repeats these functions, until the packet is delivered to the destination host.

IP will use as a default a maximum transmission unit (MTU) size of 256 octets.

NOTE: IP MTU size on a PSUEN XAT IP interface is 128 which is the same as the X.25 packet size.

IP receives 3 indications at the local network interface,

(1) an indication that the link layer is up, (used to update routing tables)

(2) an indication that the link layer is down, and that data has been received that belongs to IP (used to update routing tables), and

(3) IP processing of a received datagram,

and calls a single request.

4.2.1 IP MTU

The MTU is the largest amount of data that can be transferred across the link layer interface, and is usually determined by the underlying link layer protocol, which is the protocol layer between IP and the physical layer. That is, the MTU size of the IP interface must be less than or equal to the "send packet" size of the X.25 PVC. IP defaults to a maximum transmission unit size of 256 octets. The MTU is changeable per interface via RC/V.

The MTU includes the IP header length, which for IP version 4, when no options are included, is 20 octets. This means that maximum transport layer payload for an IP datagram is the MTU minus 20 octets, which is 236 octets. The default TCP MSS of 536 octets is based on the standard TCP header length of 20 octets.

NOTE: If the IP MTU is 256 (including IP header) and the TCP MSS is 536, then IP fragmentation will occur for TCP segments in the range of 237 to 536 (including TCP header).

4.2.2 IP ROUTING

IP Routing is used in the delivery PH to transmit the Call Data Channel (CDC) messages and Packet Data Channel (PDC) content (in the form of IP datagrams) to the Law Enforcement Agency.

Ultimately, when routing out of the switch, a destination IP address will be resolved eventually to a physical interface over which the IP datagram will be transmitted.

For the CALEA implementation, static routing is used. The static routing will be administered via RC/V.

Static routing is typically done by a network administrator entering routing commands on each individual system to which it applies. Static routes do not adjust as the network changes, and are therefore not as flexible as dynamic routing.

The individual IP routing entries will also be affected by the state of the interface at both the physical and link layer. If the link and physical layer are not up, then the routing table will be updated to indicate that that specific route is not currently usable for IP routing.

4.2.3 CDC/PDC IP ADDRESSES

CDC/PDC IP addresses provide a law enforcement agency's collection facility destination address to which call data is to be sent.

The internet protocol (IP) version 4 has been chosen to route information and content for calls being monitored by the CALEA feature set.

For CALEA, the Call Data Channel (CDC) and Packet Data Channel (PDC) will be routed from an SM or PH, through one or more switches in the packet-switched network, to the DSL connected to the law enforcement agency (LEA).

The *5ESS*® switch implementation supports IP version 4 containing a 32-bit address and a 32-bit subnet mask. The socket interface and the IP header will support only 32-bit addresses and the IP header structure itself will contain only IP addresses that are 32 bits in length.

A typical IP datagram header may look like this:

Figure 4-1 IP Datagram Header Example

4.2.4 SWITCH PROCESSORS REQUIRING IP ADDRESSES

With respect to the CALEA application, there are two subnet types within the switch:

- Inter-SM subnet consisting of all the SMs on the switch.
- Intra-SM/PH subnet consisting of all the applicable PHs in the SM and the SMP. Applicable PH types are PH3/PH4 of DSL type DSLG, X.75, X.75□, or ISM.

NOTE: The LEA monitoring station must support up to 192 simultaneous TCP connection attempts.

NOTE: The local LEA monitoring station IP address must be unique within the switch hosting the

surveillance.

Figure 4-2 gives an example of IP address assignments.

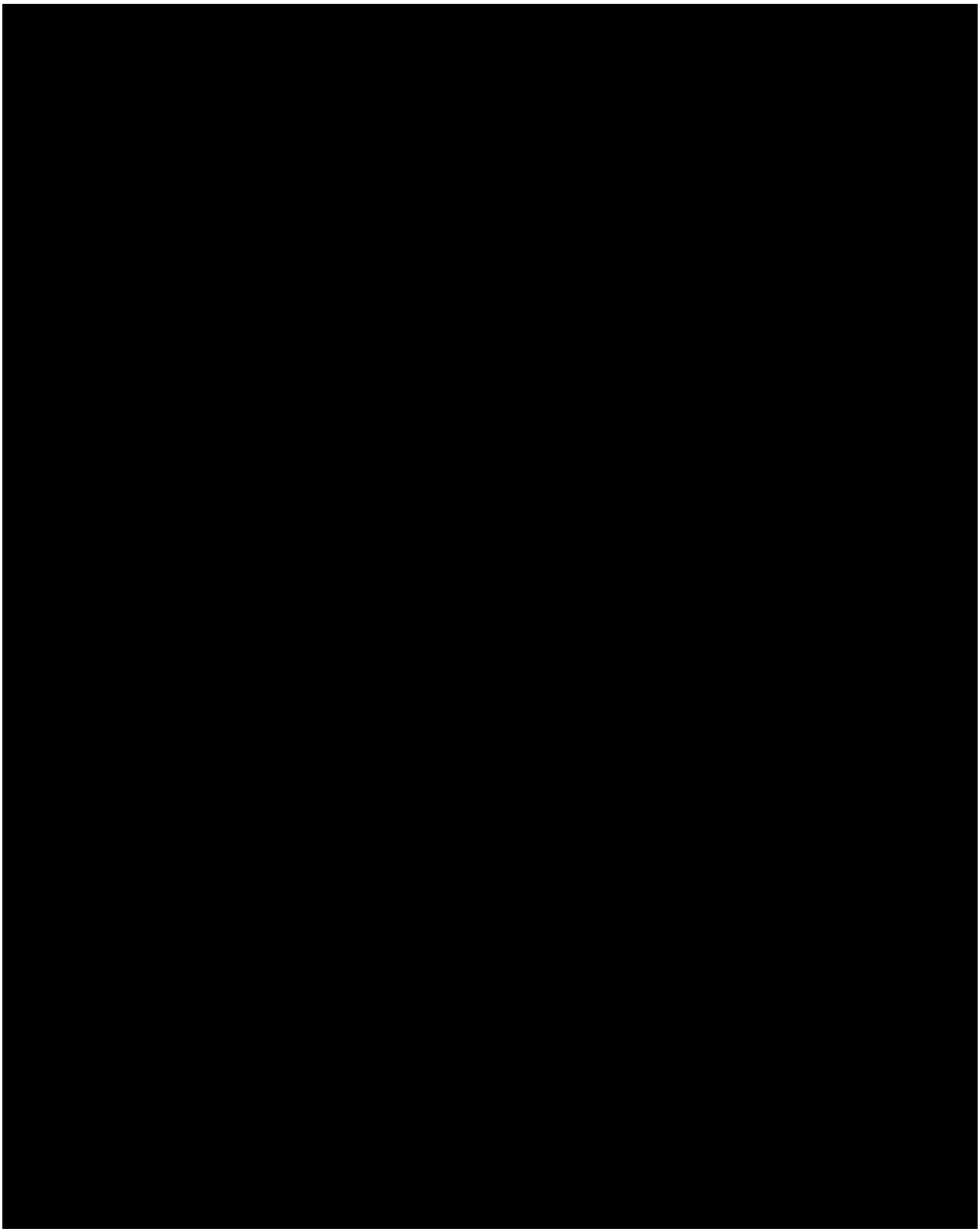

Figure 4-2 Example IP Address Assignments

4.2.5 NETWORK SECURITY AND DATA FLOW

The CALEA application may use an "intranet" network owned by the subject's service provider. For the CALEA application, the TCP/IP suite sends TCP messages via the X.25 network to the designated Law Enforcement Agency. The CALEA application shuts down the "recv" sockets interface. TCP messages are received from the Law Enforcement Agency via the X.25 network but they are not accessible.

NOTE: The *5ESS*® switch acts as the "client", while the LEA monitoring facility acts as the "server". As the "client, the switch does not grant TCP connections.

Therefore, *5ESS*® switch security issues with the CALEA application are not perceived.

Service provider-specific security measures are beyond the scope of this document. Refer to local security procedures regarding internet/intranet security.

4.2.6 TYPE OF SERVICE

Type of service is used to specify the treatment of the datagram during its transmission through the internet system. The type of service (TOS) field is tunable from the layer above, on a per IP datagram basis. A value of zero is the default. The TOS field is 8 bits wide. It is composed of a 3-bit precedence sub-field, 3 bits of service type sub-fields, and 2 unused bits.

Figure 4-3 Type of Service Field Layout

Table 4-1 Type Of Service Field Bits

Bit Number	Treatment Type	Value	Treatment Description
0-2	Precedence	111	Network Control (see Note)
		110	Internetwork Control (see Note)
		101	CRITIC/ECP
		100	Flash Override
		011	Flash
		010	Immediate
		001	Priority
		000	Routine
3	Delay	0	Normal Delay
		1	Low Delay
4	Throughput	0	Normal Throughput
		1	High Throughput
5	Reliability	0	Normal Reliability
		1	High Reliability
6	Not used	0	Reserved for future use
7	Not used	0	Reserved for future use
Note: The Network Control Precedence is intended to be used within a network only. The actual use and control of that designation is up to each network. The Internetwork Control designation is intended for use by gateway control originators only.			

4.2.7 TIME TO LIVE (TTL)

IP allows the layer above to tune the Time To Live (TTL) (also known as "hops") for each outgoing datagram. IP uses a range of TTL values from 1 to 255 hops, with 255 being the default.

4.3 ICMP

Architecturally, ICMP is layered on top of IP, using IP to carry its data end-to-end just like the transport control protocol (TCP). However, since the ICMP control protocol is such an integral part of IP, it is covered

in this chapter.

ICMP messages are sent using the basic IP header. Refer to the sample header in Section 4.2.3 . ICMP sends ICMP error messages with IP TOS equal to 0. When an ICMP error message is sent, it contains, unchanged, the first 64 octets of the IP datagram that caused the error. This includes the IP header length of 20 octets. The number of octets sent in an ICMP error message is tunable via an IP parameter function.

An ICMP error message will not be sent as a result of:

- receiving an ICMP error message,
- a datagram destined to an IP broadcast or IP multicast address, or
- receiving an IP datagram in error that is not the initial fragment.

These errored datagrams are simply discarded.

The ISDNPH always forwards outgoing IP datagrams over the BRI and/or XAT interface in a point-to-point configuration and so there is no need for receiving routing information of this type.

DESTINATION UNREACHABLE messages received by ICMP will be passed to the transport layer and will peg a counter for messages of this type. ICMP will generate a DESTINATION UNREACHABLE message with a code of 2, "Protocol unreachable" when the transport protocol is not supported. ICMP, when enabled, will also peg a count for these type of errors.

When enabled, ICMP reports to the transport layer when a SOURCE QUENCH message is received.

4.3.1 ICMP TYPE AND CODE OCTET DESCRIPTIONS

The first octet of the data portion of the ICMP datagram is a ICMP "Type" field. The value of this field determines the format of the remaining data. The CALEA application supports the following:

Type	Code	Description	Query	Error	TCP Aborts Connection Attempts
0	0	echo reply (Ping reply)	X		
3		destination unreachable		Yes	
	0	network unreachable		X	
	1	host unreachable		X	
	2	protocol unreachable		X	
	3	port unreachable		X	
	4	fragmentation needed but don't-fragment bit set		X	
	5	source route failed		X	
	6	destination network unknown		X	
	7	destination host unknown		X	
	8	source host isolated		X	
	9	destination network administratively prohibited		X	
	10	destination host administratively prohibited		X	
	11	network unreachable for TOS		X	
	12	host unreachable for TOS		X	
	13	communication administratively prohibited by filtering		X	
	14	host precedence violation		X	

	15	precedence cutoff in effect	X
4	0	source quench	X
8	0	echo request	X
11		time exceeded:	No
	0	time-to-live equals 0 during transit	X
	1	time-to-live equals 0 during reassembly	X
12		parameter problem:	No
	0	IP header bad (catchall error)	X
	1	required option missing	X
13	0	timestamp request	X
14	0	timestamp reply	X
17	0	address mask request	X
18	0	address mask reply	X

4.3.2 ICMP MESSAGE LAYOUTS

A value of 1 in the 8-bit protocol field in the IP header indicates ICMP. A template ICMP header looks like this:

Figure 4-4 ICMP Header Example

Following are samples of ICMP headers for various type/code combinations defined in the table in Section 4.3.1 .

Figure 4-5 Echo Request/Reply Message Header

Figure 4-6 Address Mask Request/Reply Message Header

Figure 4-7 Timestamp Request/Reply Message Header

Figure 4-8 Destination Unreachable Message Header

Figure 4-9 Source Quench Message Header

Figure 4-10 Time Exceeded Message Header

Figure 4-11 Parameter Problem Message Header

5. TRANSPORT LAYER - TCP

5.1 OVERVIEW

Layer 4, the transport layer, provides a highly reliable, end-to-end connection for communication between two processes and manages error correction and reassembly of out-of-order packets. That is, if a data unit is lost and retransmitted, it may arrive out of order, so Layer 4 is responsible for reassembling data units back into the correct order.

For the purposes of the CALEA application, TCP comprises the transport layer.

5.2 TCP OVERVIEW

TCP maps an incoming IP segment to the appropriate socket and, therefore, the application layer. TCP is a Layer 4 error recovery protocol used by the endpoints of an Internet connection to ensure the accurate delivery and receipt of packets. This is done by accessing the appropriate Protocol Control Block (PCB) for each incoming IP datagram, using the key fields: local and foreign IP addresses and the local and foreign port numbers, to map to a specific socket. The resulting segment to be sent on the application layer has a default maximum segment size (MSS) of 536 octets (including the 20 octet TCP header). The actual range is 108 to 64K and is tunable per socket interface.

TCP tracks packets by sequence numbers. For example, when a sending host sends 100 bytes, it informs the receiving host of the info being sent. When the receiving host receives the 100 bytes, its TCP software sends an acknowledgement to the sending host. This tells the sending host that it may send more data. If the sending host does NOT receive an acknowledgement within a certain time-out period, then it re-transmits the 100 bytes. This continues until the sending host receives an acknowledgement of receipt, or the maximum number of retries (default = 12) is exceeded. A checksum is added to each segment transmitted. The receiving user checks the checksum and discards any damaged segments.

If a user needs confirmation that all data has been transmitted, a "push" function is defined; that is, the data is to be pushed through to the receiving user. However, there is no guarantee or confirmation of immediate delivery.

TCP also provides a way for the receiver to control the amount of data that will be accepted from the sender. With each acknowledgement (ACK) sent back to the sender, a "window" is returned indicating how much more data (in the form of a range of sequence numbers) will be accepted by the receiver in the next segment sent. Note that indicating a large window size encourages transmissions; however, if more data arrives than can be accepted, it will be discarded. On the other hand, indicating a too-small window size restricts data transmission to the point of creating roundtrip delay between each new segment sent.

To allow for multiplexing within a single host, TCP provides a set of addresses or ports within each host. When concatenated with the network and host addresses from the internet communication layer, a connection-oriented socket is formed. A pair of sockets uniquely identifies each connection. A connection includes not only sockets, but sequence numbers and window sizes. When two processes have completed communication over a connection, the connection is closed and the resources are freed for other uses.

5.3 CALEA USE OF TCP

The CALEA application uses a deployment of the TCP/IP platform on the ISDNPH (both Delivery PH and non-Delivery PH) running on the PH3 and/or PH4. The CALEA feature set also uses a deployment of the TCP/IP platform on the SMP, running on the SMP20 = 68020 (SM); SMP40 = 68040 (SM2000 SM); and/or SMP60 = 68060 (SM2000 SM).

The CALEA application uses an "intranet" network owned by the subject's service provider. For the CALEA application, the TCP/IP suite sends TCP messages via the X.25 network to the designated Law Enforcement Agency. The CALEA application shuts down the "recv" sockets interface. TCP messages are received from the Law Enforcement Agency via the X.25 network but they are not accessible.

NOTE: The switch expects data in network byte order.

TCP reports any received ICMP error messages to the appropriate application above, but will not necessarily abort the connection due to these errors. If the connection is aborted, TCP will notify the associated layer. See the Section 4.3 for a description of ICMP functionality and a listing of ICMP error messages and their meanings.

Segments may also be lost due to errors resulting from checksum test failures or network congestion. To combat this, TCP uses retransmission to ensure segment delivery. This sometimes results in duplicate segments being received (which is covered later in this chapter). TCP, when retransmitting, implements the "Jacobson Slow Start Algorithm" and the "Jacobson Congestion-Avoidance Algorithm", as stated in RFC 1122. The maximum number of TCP retransmissions for a SYN/non-SYN TCP segment is 12. When calculating round trip delay, TCP implements the "Karn's Algorithm" (RFC 1122) in order to calculate the retransmission timeout (in milliseconds), and Jacobson's algorithm for calculating the round-trip time, which measures the time from when a segment is sent until the time that it is acknowledged. TCP will pass the following ICMP messages to the associated application layer above, but ***will NOT*** abort the connection because of the following ICMP error messages:

- Time Exceeded (Type 11),
- Parameter Problem (Type 12),
- Destination Unreachable (Type 3) with a code of 0, 1, or 5.

TCP ***will not*** abort the current connection due to an ICMP error message of Destination Unreachable (Type 3) with a code of 2, 3, or 4. However, TCP ***will*** abort a new connection attempt.

5.4 TCP FUNCTIONAL SPECIFICATION

5.4.1 HEADER FORMAT

TCP segments are sent as datagrams, which already have an IP header including the source and destination host addresses. The TCP header follows the IP header, supplying TCP-specific information. A typical TCP header looks something like this:

Figure 5-1 TCP Header Example

The fields in the TCP header are defined in Table 5-1 .

Table 5-1 TCP Header Fields

FIELD	SIZE	DEFINITION
Source Port	16 bits	Source port number
Destination Port	16 bits	Destination port number
Sequence Number	32 bits	Sequence number of the first data octet in this segment (except when SYN is present; then it is the initial sequence number and the first data octet is ISN+1)
Acknowledgement Number	32 bits	If the ACK control bit is set, this field contains the next sequence number the send of the segment is expecting to receive.
Data Offset	4 bits	The number of 32-bit words in the TCP header. This indicates where the data begins.
Reserved	6 bits	Reserved for future use...must be zero.
Control bits	6 bits	URG: urgent pointer field significant (NOT SUPPORTED) ACK: acknowledgement field significant PSH: push function RST: reset the connection SYN: synchronize sequence numbers FIN: no more data from sender
Window	16 bits	Number of data octets, beginning with the one in the Acknowledgement Number field, which the sender is willing to accept.
Checksum	16 bits	The checksum field is the 16 one's complement of the one's complement sum of all 16-bit words in the header and text.
Urgent Pointer	16 bits	When the URG control bit is set, this points to the sequence number of the octet following the urgent data.
Options	variable	Options are multiples of 8 bits in length.

Refer to RFC 793, Transmission Control Protocol, for in-depth information regarding these fields.

5.4.2 SEQUENCE NUMBER RANGE

Every octet of data sent over a TCP connection has a sequence number such that each individual octet can be acknowledged. The acknowledgement mechanism is cumulative and the actual sequence number space is finite, the range being 0 to 2**32 - 1. All arithmetic dealing with sequence numbers must be performed modulo 2**32.

5.4.3 PROCESSING TIMES

The TCP/IP feature of the CALEA application is directly responsible for processing times due to the IP, TCP, and the socket interface. It is not responsible for the processing times due to the supporting layers below IP, or the processing times due to the socket applications.

5.4.4 CONNECTION PROGRESSION

Figure 5-2 explains the sequence of events throughout a surveillance, from the beginning of a call surveillance, to the end.

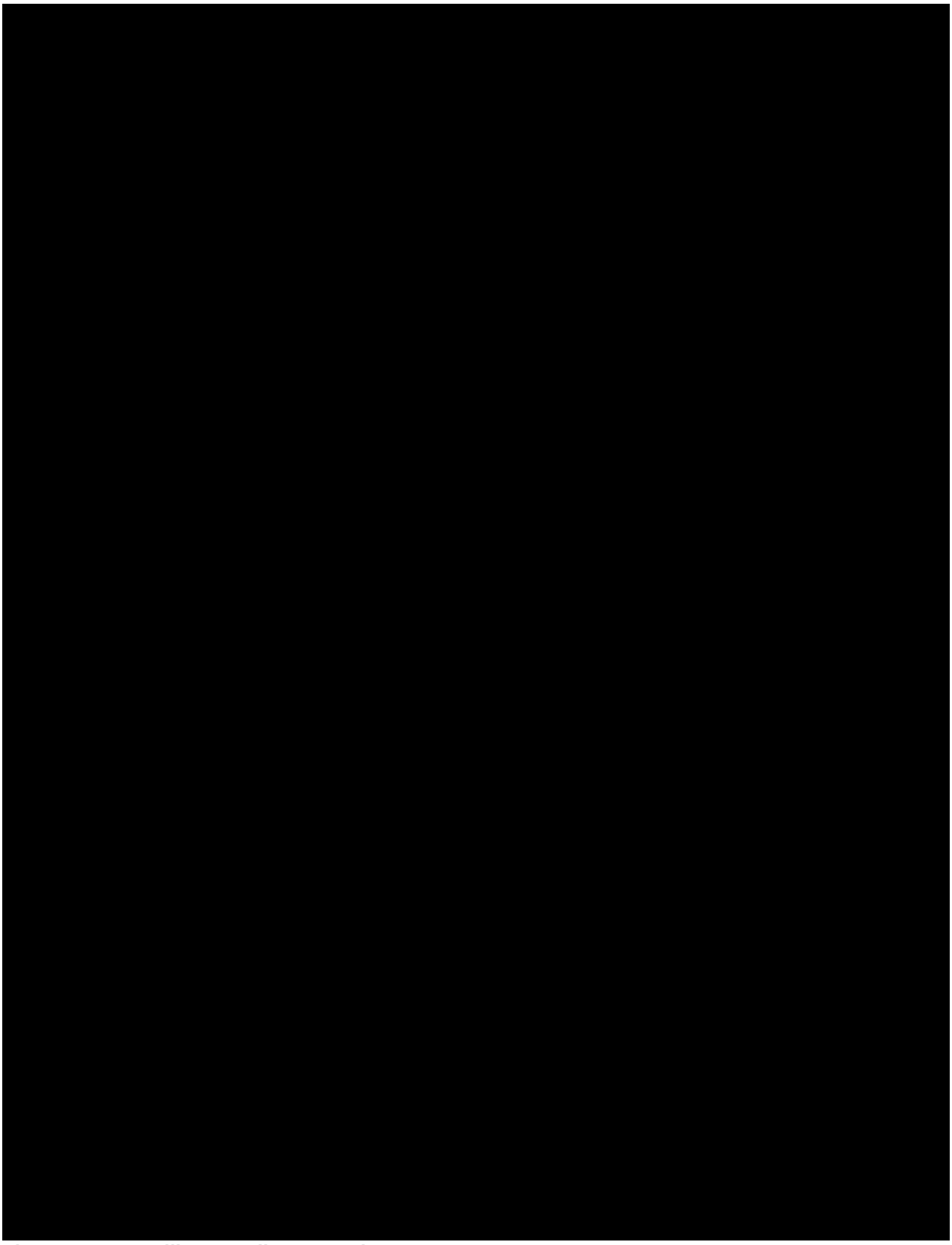

Figure 5-2 Surveillance Call Progression

5.5 SOCKETS INTERFACE TO THE APPLICATION LAYER

Sockets is a widely used interface between the TCP/IP network and the application program. A socket is a path that is defined by a pair of addresses, namely the local internet protocol (IP) address and port number for TCP and the foreign IP address and port number. Each address/port combination is referred to as a "socket address," and both address/port combinations are also referred to as a "socket pair" of addresses. When the socket interface requests action or information from an underlying protocol, a user request will be issued to the target protocol. The sockets interface will not attempt to directly access data under the domain of a protocol.

6. GR-30 CDC VOICEBAND DATA TRANSMISSION

6.1 GR-30 ANALOG LINE TERMINATION □ PHYSICAL LAYER

The physical layer specification for an analog line termination for CDC message transmission is a subset of the requirements in the Telcordia GR-30-CORE, Issue 2, Dec., 1998 document, section 2.5 and in the ANSI T1.401-1993 Standard. This analog line interface is provided by the CDC Using Voiceband Data Transmission feature (99-5E-8318) and is available in the 5E16.2FR1 software release.

The CDC messages are transmitted over the voice band portion of a connection dialed out from the IAP to the CB. The connection may pass through tandem trunks. The typical CB interface may be a properly terminated analog 2-wire line (loop or ground start), ISDN B-channel provisioned for voice, or any other suitable network termination that does not impair the FSK or DTMF voice band transmission. Figure 6-1 shows the line and trunk interfaces.

Figure 6-1 Voice Band CDC Transmission

The CB may take the link down at any time by releasing its side of the call (e.g. going on-hook). It is expected that the CB will, in turn, release the connection when the IAP takes the link down. The CB line needs to detect disconnect from the IAP. Since the link can stay up with no carrier presented (i.e. no CDC messages being transmitted), the CB cannot rely on carrier sensing. Some recommended procedures for the CB detecting disconnect with an analog line are:

(1) Use a ground start line to receive a positive idle signal.

(2) Use a loop start line that detects disconnect by either (or both) of these methods:

  (1) Sense 800ms open interval disconnect signal.

  This signal is sent to terminating answered calls that remain off-hook after the originator hangs up. This signal is also sent to terminating unanswered calls that received power ringing.

  (2) Detect dial-tone after re-origination.

  If dial-tone detection is used, the line may not have any feature assigned that blocks dial-tone re-application such as denied origination or Modified Calling Line Disconnect procedure. The dial-tone detector must not be falsely triggered by GR30 FSK frequencies.

(3) Disconnect on lack of message activity. The IAP will reconnect when messages are ready to send.

This can be used in combination with **1** and **2**.

NOTE: If an ISDN B-channel provisioned for voice is used as the CB interface, the signaling protocol provides a clear disconnect signal and the concerns of the previous paragraph are eliminated.

The physical characteristics of the analog line interface are defined in T1.401-1993; Section 5 details loop-start signaling characteristics and Section 6 details ground start signaling. The interface must be set up to use DTMF signaling. Section 7.2 of T1.401-1993 details DTMF signal frequencies, power, and timing requirements for use as network control signals in the US telephone network.

Signalling for this interface uses the low-speed (1200 bps) Frequency Shift Keying (FSK) described in section 2.5 of Telcordia GR-30-CORE. The off-hook protocol is used except that the CPE Alerting Signal (CAS) and the Subscriber Alerting Signal (SAS) are not used.

The IAP expects the CB to respond, when optionally provisioned, using DTMF signal digits. DTMF Signal Digits are DTMF digits in the range of 0-9 played for 50-70 ms minimum followed by 50-70 ms minimum of silence. The following signals used below (NACK, ACK, and login ID) are all defined as DTMF signal digits.

- The ACK (ACKnowledgement) signal is a DTMF 0 Signal Digit.
- The NACK (negative ACKnowledgement) signal is added as a DTMF 1 Signal Digit.
- The CB must wait at least 250 milliseconds and no more than 0-5 seconds (as provisioned) after receiving the last CDC packet of a CDC message before sending an ACK/NACK to the IAP.
- The IAP must wait at least 250 milliseconds after receiving the end of any DTMF digit (ACK/NACK signal or login digit) before sending a subsequent CDC message to the CB.
- The IAP will silently wait at least 100 milliseconds after sending each CDC packet.
- ACK/NACK signals are optionally sent from CB to IAP at the end of each CDC message.
- The login ID is a set of 3 DTMF Signal Digits with values from 0-9. The range of valid login ID's is 000 to 999.

The IAP can also be provisioned with a switch-wide login ID of 3 digits. If the login ID is provisioned and if the IAP is requested, the IAP will send the CB a login message requesting the CB to send the login ID.

6.2 GR-30 DATA LINK LAYER

The GR-30 based analog line interface can be used to transmit CDC messages. This interface is provided by the CDC Using Voiceband Data Transmission feature (99-5E-8318).

The data link layer takes each message format and creates a message frame by prepending a preamble sequence and appending a checksum word. The data link layer is also responsible for framing each byte. The message frame preamble consists of either Channel Seizure Signal and the Mark Signal, or only the Mark Signal. The purpose of the Channel Seizure Signal and the Mark Signal is to alert and condition the CPE for reception of a message frame. The purpose of a checksum word is to provide the CPE with a means for error detection.

The data link layer specification used is a subset of the requirements in GR-30-CORE, Section 2.4. A CDC message is transmitted from the IAP to the CB in one or more CDC packets, which are Single Data Message Format (SDMF) frames using off-hook data transmission.

6.2.1 FRAMING AND ORDERING OF BITS AND BYTES

Each message byte in the SDMF is preceded by a start bit (space) and followed by a stop bit (mark). The least significant bit of each message byte is transmitted first for SDMF.

6.2.2 PREAMBLE SEQUENCE FOR OFF-HOOK DATA TRANSMISSION

Each SDMF frame is preceded by a Mark signal. The Mark signal consists of 80 bits of continuous mark.

6.2.3 ADDITIONAL MARK BITS

This interface requires that there be no additional mark bits between words in the SDMF.

6.2.4 ERROR DETECTION

The transmitter computes a checksum word for SDMF messages according to a specific algorithm and appends it to the message. At the receiver, the checksum word is recomputed and compared to the checksum word sent in the message frame. The received message is considered to be error free if both values are identical.

NOTE: This approach cannot detect all transmission errors. Specifically, it cannot detect offsetting bit errors occurring in the same message. Error correction is not supported by this protocol.

The last word of all Single Data Message Frames is a checksum word. The checksum word contains the two's complement of the modulo 256 of the binary representation sum of all the other words in the message (i.e., message type, message length and message data words for the SDMF).

The stop bit following the checksum word (of a Single Data message) is transmitted completely and shall either be continued so that the data signal is stopped at a zero crossing or shall be followed by an additional one to 10 mark bits.

6.3 GR-30 MESSAGE ASSEMBLY LAYER

The following is a description of the SDMF frame, known in this context as a CDC packet, that carries part or all of a CDC message.

6.3.1 SINGLE MESSAGE DATA FORMAT (SDMF)

The SDMF consists of a message type, a message length, and one or more message words.

The message type, message length, and each message word is an 8-bit byte.

The message type word in SDMF contains the 8-bit value assigned to the feature whose data is being sent to the customer.

NOTE: Section 7.1 of T1.401.03 defines two message type words: Caller Name Display (CND) with a value of 4, and Visual Message Waiting Indicator (VMWI) with a value of 6. This interface sets the message type word in all CDC packets to CND (Hexadecimal 4).

The message length word in SDMF contains the 8-bit binary representation of the number of words in the message following it, excluding the checksum word. For the SDMF, the message length shall be equal to the total number of message data words.

6.3.2 MESSAGE WORD

The message data (collection of message words) portion of a CDC packet has two fields - the CALEA Message Type and the CDC Message Data:

CALEA Message Type (8 bits). Four message types are used for this interface:

CALEA CDC Begin Packet (ASCII '*' = Hexadecimal 2A) CALEA CDC Continue Packet (ASCII + = Hexadecimal 2B) CALEA CDC End Packet (ASCII '#' = Hexadecimal 23) CALEA CDC Solo Packet (ASCII '$' = Hexadecimal 24)

The CDC Message Data is sent using Lucent ASN.1 CDC Format. This interface specifies the extension of the CDC ConnectionTest message to include the reporting of autonomous surveillance-related events, including the GR30 login and heartbeat events.

6.3.3 MESSAGE SEGMENTATION/REASSEMBLY

The IAP assumes that it always originates message transmission to the CB. It will always dial out to the CB. The CB must return answer supervision to the IAP when called. Once the call is in the talking state, CDC messages may be transmitted.

The IAP assumes that it always originates message transmission to the CB. It will always dial out to the CB. The CB must return answer supervision to the IAP when called. Once the call is in the talking state, CDC messages may be transmitted.

Timers are provisionable on the IAP only. There is no defined interface for the CB to change the IAP timers.

- T1 (fixed on IAP) - maximum time to await login attempt (in sec.): **5** seconds fixed.
- T2 (provisionable on IAP per GR-30 link) - maximum time to await ACK/NACK after sending CDC End Message packet: 0-5 sec provisionable, default value of **0** sec. Note on intent: The timer will be started after the last packet of the CDC message is sent. The IAP expects the ACK/NACK to be sent only after all CDC packets for a CDC message have been sent. It determines how long the IAP should wait for the ACK or NACK from the collection box. If the timer expires, the IAP will resend the CDC message up to the C1 limit. If T2 is provisioned to 0 on the IAP, no ACK/NACK expected by IAP for any message.
- T3 (provisionable on switch wide basis) - timer for IAP sending heartbeat messages during inactivity: 0-60 minutes, default value of **0**. This timer determines how often the IAP has to send the heart beat message (see section 6 for format) to the collection box when link is idle. When the timer expires, the IAP will send a heart beat message to the collection box. If T3 is provisioned to 0 on the IAP, the IAP will not send heartbeat messages.
- T4 (provisionable on IAP per GR-30 link) - minimum time to retry sending a failed pending CDC message: 5-255 seconds, default value of **5** sec. This timer is used to await a transient fault to clear before re-establishing the GR-30 connection.
- T5 (provisioned with Recent Change) - amount of time without IAP or CB response before IAP starts to discard CDC messages: initial value of **240 minutes**, user accessible range 0-240 minutes in 30 minute intervals (i.e. 0, 30, 60, 90 ... 240). When T5 is either set to 0 or expires, CDC messages will be discarded after being displayed to security technician. If T5 is reset by user while display/discard is in progress, display/discard will be postponed until T5 expires. The messages are sent to the CALEA ROP and then discarded from the CDC message buffer at a rate of one CDC message per 30 seconds (approximately) until all buffered messages are discarded.

The following is a list of counters:

- C1 (fixed on IAP) - maximum number of transmission attempts before discarding CDC message - C1 is incremented and retransmission is attempted when either a NACK is received by the IAP or Timer T2 expires: fixed at **3**
- C2 (fixed on IAP) - maximum number of consecutively discarded messages before taking GR-30 link down; that is, the number of times C1 is exceeded before assuming the link or transmission is bad:

fixed at **3**

- C3 (fixed on IAP) - maximum number of link establishment attempts before taking down the GR-30 CDC link with the assumption the link is bad and should not be retried: fixed at **3**.

The following is a list of pointers:

- CDC Packet - a complete or partial CDC message sent in a Single Data Message Format (SDMF) frame. A SDMF frame can have from 1 to 255 payload bytes. However, in case that a IAP implementation cannot send a maximal SDMF message or a CDC message exceeds 255 bytes, the IAP shall send a fragment of the CDC message to the CB. The IAP shall send (fragments of) CDC messages in strict FIFO order. That is, the IAP shall send (the fragments in order of) a CDC message. The intent is to allow the CB to "reassemble" the CDC fragments by buffering and concatenating CDC fragments until a complete CDC message is received.

- DTMF X Signal Digit - DTMF digit X's (X in the range 0-9) signal played for 50 ms minimum followed by a minimum of 50ms of silence. Additionally, premises DTMF signals, DTMF frequency tolerances, and power are defined in Telcordia GR-506-CORE, Issue 1, Nov., 1996. It is an objective to keep signal digit play and silence intervals to a minimum.

- ACK (ACKnowledgement) - An ACK signal is a DTMF 0 Signal Digit. ACK/NACK signals are expected by the IAP if Timer T2 is provisioned to a non-zero value. If T2 is provisioned to 0 on the IAP, the IAP does not expect ACK/NACK for any CDC message.

- NACK (Negative ACKnowledgement) - A NACK signal is a DTMF 1 Signal Digit. ACK/NACK signals are expected by the IAP if Timer T2 is provisioned to a non-zero value. If T2 is provisioned to 0 on the IAP, the IAP does not expect ACK/NACK for any CDC message. If a CDC message is NACK'd, the entire CDC message will be retransmitted.

- Login ID - IAP's ID = a sequence of 3 DTMF Signal Digits (a unique office-wide value). Optionally provisioned on the IAP. The range of valid login ID's is 000 to 999.

- Future Use - DTMF * and # Signal Digits are reserved for future use. They will not be sent by the IAP and ignored if received by the IAP. Note that DTMF * and # Signal Digits are not the same as CALEA Message Types * and # - DTMF Signal Digits are for IAP/CB link signaling, where as CALEA Message Types are used for packet assembly/reassembly.

- Login Message - a pre-formatted CDC ConnectionTest message requesting the CB to send its login ID to the IAP (see Section 6 for format). The IAP keeps track of the login status in a "link verification" field. This message is optionally sent by IAP depending on IAP provisioning.

- Heart Beat Message - a pre-formatted CDC ConnectionTest message (see Section 6 for switch-generated format) used to keep the link alive. Heart Beat Messages are sent by the IAP if Timer T3 is provisioned to a non-zero value. If T3 is provisioned to 0 on the IAP, the IAP will keep the link up without sending Heart Beat messages.

  A summary of the IAPs behavior is provided in the Figure 6-2 and associated Table 6-1 :

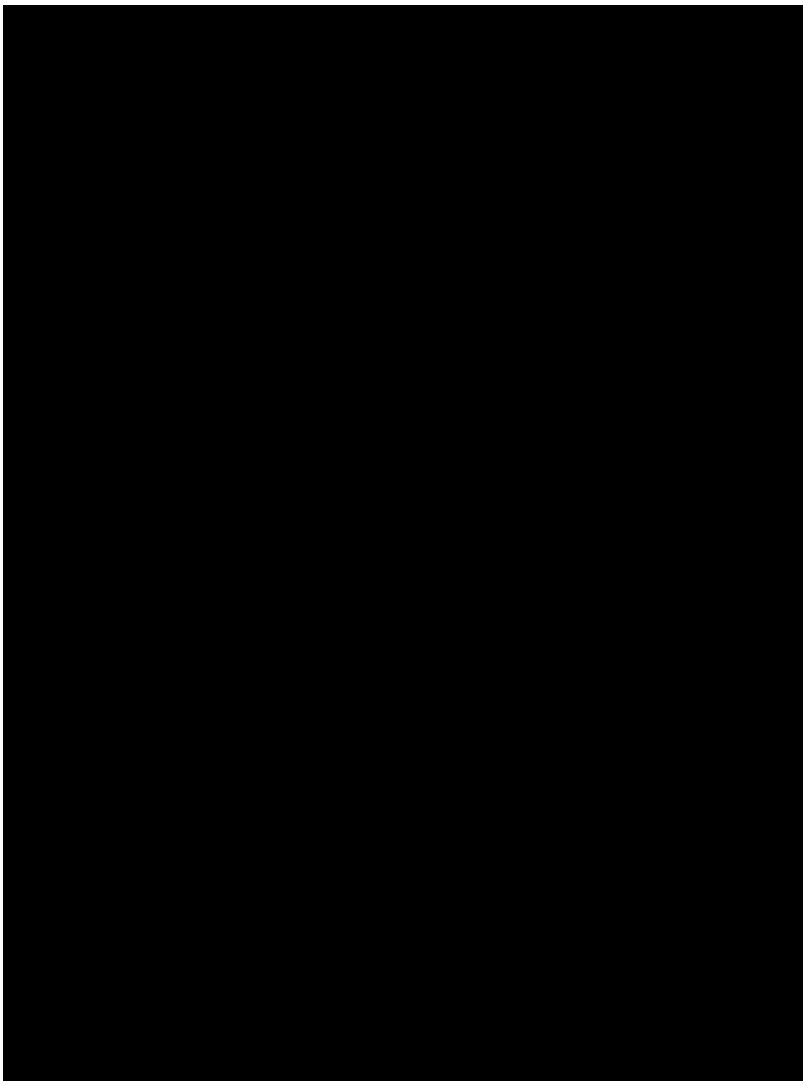

Figure 6-2 IAP Behavior

Table 6-1 Summary of IAP Actions

Summary of IAP Actions	
Label	Input
A	Stop Timer T5
B1	Remove "Clear Timer T5"
B2	Timer T5 (Link Down) expires. Pending DCD messages in buffer
B3	Request to set Timer T5's value to X minutes.
C	Stop Timer T4
D1	Start Timer T4
D2	Start Timer T5, remove "Reset Timer T4"
E1	Stop Timer T3, Start Timer T2
E2	Re-start Timer T3
F1	Start Timer T3, remove "Reset Timer T3"
F2	Start Timer T2, Start Timer T3 (or Re-start if already active)"
G1	Start Timer T1, Re-start Timer T3
G2	Re-start Timer T3
H,I	Stop Timer T1
K	Timer T1 Fires
L1	Start Timer T3, Stop Timer T2
L2	Start Timer T1, Stop Timer T2
M1	Re-start Timer T2
M2	Stop Timer T2, Start Timer T5, Stop all other timers
N1	Re-start Timer T2
N2	Start Timer T5, Stop all other timers
O,P	Start Timer T5, Stop and active timers

The following describes the initial conditions the IAP assumes for each state:

State	Initial Setup
Init	Link validation = "not active". All timers inactive. All counters = 0.
Wait Answer	Guarded by call processing "wait for answer" timers.
Trans	Set Timer T3 (heartbeat).
Login	Set Timer T1 (login).
Wait ACK	Set Timer T2 (ACK).

6.3.4 IAP Message Segmentation Description

The IAP is assumed to have a limited data buffer size to send CDC data to the CB. The IAP will send the CDC packets in strict First-In First Out (FIFO) order. That is, the IAP will fragment the message if it cannot fit the entire CDC message into one outbound data buffer. It will send the fragments to the CB in order of a CDC message and await the entire CDC message's acknowledgement, if so provisioned, before starting to send the next CDC message. The intent is to allow the CB to "reassemble" the CDC packets by buffering and concatenating CDC packets until a complete CDC message is received. Each CDC packet will be encoded, as described above, using SDMF - Table 6-2 shows the format of the CDC packet used by the IAP (in time order):

Table 6-2 CDC Packet Layout

Field	Subfields (if any)	CDC Packet Layout
Message Type		8 bits per GR-30. Set to Calling Name Display (CND) SDMF Message Type value of Hexadecimal 04.
Message Length		8 bits. Set to the number of bytes in the CDC Message. Specifically, it excludes the Checksum.
CDC Message Data		The CDC message data field has two subfields - the CALEA Message Type and CDC Data.
	CALEA Message TypeSubfield	8 bits per GR-30. The following message types are defined in this interface: + CALEA CDC Begin Packet (ASCII "*" = Hexadecimal 2A). + CALEA CDC Continue Packet (ASCII "+" = Hexadecimal 2B), + CALEA CDC End Packet (ASCII "#" = Hexadecimal 23), and + CALEA CDC Solo Packet (ASCII "$" = Hexadecimal 24).
	CDC DataSubfield	A (fragment of a) CDC message in Lucent ASN.1 CDC Format.
Checksum		8 bits - The checksum word shall contain the two's complement of the modulo 256 of the binary representation sum of all the other words in the message, including overhead words.

The first byte of the CDC message data shall contain the CALEA Message Type Word subfield. The IAP sets the CALEA Message Type word as follows:

- If a CDC packet completely contains a whole CDC message, the CDC packet's CALEA Message Type word will be set to "CALEA CDC Solo Packet" (ASCII "$" = Hexadecimal 24).
- The CALEA Message Type word of the first of multiple CDC packets will be set to "CALEA CDC Begin Packet" (ASCII "*" = Hexadecimal 2A).
- The CALEA Message Type word of the last of multiple CDC packets will be set to "CALEA CDC End Packet" (ASCII "#" = Hexadecimal 23).
- All CDC packets except the first/only and last will have their CALEA Message Type words to "CALEA CDC Continue Packet" (ASCII "+" = Hexadecimal 2B)

Number of CDC Packets/CDC Message	CALEA Message Type Word(s) (separated by spaces)
1	$
2	*#
3	*+#
5	* + + + #
8	* + + + + + + #
10	* + + + + + + + + #
12	* + + + + + + + + + + #

The IAP can be provisioned to expect ACK/NACK from the collection box for each CDC message sent. If so provisioned, the IAP will await an acknowledgement before starting to send the next CDC message. The CB would respond with an ACK if the CDC message could be assembled from the CDC packet(s) and the checksum(s) were correct for all CDC packets used to send the CDC message, and NACK for the first failing CDC packet otherwise. The NACK 1 signal digit represents the fact that the CB has determined any or all CDC packets are in error. The CB should wait until receiving the final (or only) CDC packet before NACK'ing the CDC message.

7. APPLICATION LAYER

7.1 OVERVIEW

The Application Layer is the top layer of the Internet protocol suite. It combines the Presentation and Application layers of the OSI model. This layer deals with taking the reassembled data streams and directing them to the CALEA application.

NOTE: The *5ESS*® switch acts as the "client", while the LEA monitoring facility acts as the "server".

7.2 TPKT

Data from the CDC message-generating software in the SM and the PDC packet-generating software in the PH is encapsulated in a TCP packet (TPKT) header. The resultant "TCP packet" is transmitted to the law enforcement agency IP network destination.

NOTE: The exclusion of the TPKT header is provisionable on a per switch basis. So it is possible for a LEA collection facility to receive packets that do not contain TPKT headers. A LEA collection facility that receives messages from multiple *5ESS*® switches may be required to accept CDC messages from one switch that include the TPKT Header, while a subsequent switch sends CDC messages that do not include the TPKT header. Provisioning options must be arranged with the specific LEA.

A typical TPKT header looks like this:

Figure 7-1 TPKT Header Example

When sending the Transport Protocol Data Unit (TPDU) to Transport Control Protocol (TCP) for CDC messages and PDC packets, the switch populates the packet length field of the TCP Packet (TPKT) header with the TPDU size. The fields in the header are as follows:

- Octet 1 is the version field (version number), which is set to "3".
- Octet 2 is a reserved field and is populated with "0".
- Octets 3 and 4 contain the packet length, which includes the header and the data. It is between 7 octets and 65535 octets long.

For CDC messages, Abstract Notation One (ASN.1) encoding (as defined in ITU-T Recommendation X.209) provides the length of the CDC message for the TPDU size.

For PDC packets, the size is determined by the size of the X.25 packet.

7.3 CDC

7.3.1 CDC MESSAGE ENCODING

The CDC carries information regarding the intercept subject and call-identifying information for circuit-switched and packet-switched calls from the switch to the LEA. All CDC messages sent to the law enforcement monitoring facilities are encapsulated into TCP/IP messages, that is, encoded to be binary-compatible with ITU-T Recommendation X.208, Abstract Notation One (ASN.1) and ITU-T Recommendation X.209, Basic Encoding Rules. When a call event is mapped to a CDC message, the message fields are populated and encoded as specified by the LAES profile and a TPKT header added before sending the message on.

The first octet of the ASN.1 message (after TCP/IP header,etc.) defines which CDC message is being sent and starts with **0xy**, where **y** may be

- **A1** – Answer
- **A2** – CCClose
- **A3** – CCOpen
- **A4** – Change
- **A5** – Origination
- **A7** – Redirection
- **A8** – Release
- **AA** – TerminationAttempt
- **AB** – ConnectionTest
- **AD** – Connection
- **AE** – ConnectionBreak
- **AF** – DialedDigitExtraction
- **B0** – NetworkSignal
- **B1** – SubjectSignal

7.3.2 CDC MESSAGE TRANSMISSION TIMING

If the CDC interface over which a CDC message is to be sent is transmission ready, the CDC message must be sent within 3 seconds after the call event to which it applies.

Exceptions to this timing constraint include:

- The DialedDigitExtraction message must be sent within 23 seconds after the call event to which it applies.
- The NetworkSignal message must be sent within 10 seconds after the call event to which it applies.
- The Connection and ConnectionBreak messages must be sent within 3 seconds after the call event to which it applies.
- The SubjectSignal message must be sent within 23 seconds after the call event to which it applies.

7.3.3 CDC MESSAGE DEFINITIONS

Table 7-1 lists all CDC messages supported for the *5ESS*® switch wireline implementation of the CALEA application. Each message is followed by a table containing (1) the parameters that make up the message, (2) the requirement for each parameter:

- Mandatory (M) – must be provided in every instance of the message
- Optional (O) – may be provided if the service provider decides to deliver this information
- Condition (C) – must be provided under certain conditions, otherwise it is not provided,

and (3) the usage of each parameter.

NOTE: The LAESMessage defines all other CDC messages, therefore it does not contain the MOC requirement.

- LAESMessage - defines the LAES messages

Table 7-1 LAES Messages and Definitions

Message	Usage
Answer	Reports that a connection-oriented call or leg has been answered.
CCClose	Reports the end of call content delivery on the CCC or PDC.
CCOpen	Reports the beginning of call content delivery on the CCC or PDC.
Change	Reports merging or splitting of connection-oriented call identities.
Origination	Reports authorized connection-oriented call origination attempts or number translations for the intercept subject performed by the Access function.
PacketEnvelope	**NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**
Redirection	Indicates that an incoming connection-oriented call attempt, originally directed toward the subject, has been redirected by the subject.
Release	Reports that a connection-oriented call has been released.
ServingSystem	**NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**
TerminationAttempt	Reports a connection-oriented call termination attempt.
ConnectionTest	Sent to verify the connectivity of the CDC. Beginning with the 5E16.2 software release, this message is also used as a heart beat message and as a login message.
Connection (5E15 and later) **a**	Reports the addition of one or more parties to a conference call.
ConnectionBreak (5E15 and later) **a**	Reports the removal of one or more parties from a conference call.
NetworkSignal (5E15 and later) **a**	Reports 1. call progress tones (busy/reorder) for incomplete calls originated by the subject, 2. audible, visual, out-of-band signaling for incoming call attempts to a subject (includes analog Calling Name, Calling Number, Q.931 Display IEs), and 3. call waiting and message waiting indications sent to a subject by the switch.
SubjectSignal (5E15 and later) **a**	Reports subject-initiated signals to control feature/service operation (for example, call waiting or call forwarding). The signal may be in-band or out-of-band, and may be call-associated or non-call-associated (such as flash and feature keys).
DialedDigitExtraction (5E15 and later) **a**	Reports subject-dialed digits for all Level I and Level II subject-originated calls, or when a call is connected to another telecommunication service provider's service for processing and routing.

Notes:

a. The DC District Court of Appeals ruled in August 2000 that the FCC has not provided adequate justification for these messages to be included in the revised industry CALEA standard, J-STD-025A. Subsequent to the FCC response to the Court's directive, and further ruling by the Court of Appeals, there is no CALEA standards mandate to provide this information to Law Enforcement. Therefore, each message may be provisioned off (mark the fields as "N" on RC/V view C.2) at the discretion of the Service Provider.

- Table 7-2 defines the parameters of the Answer message.

Table 7-2 Answer Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
AnsweringPartyIdentity	C	Include, when known, to identify the answering party or agent. Answering Party ID is sent even if it is the same as the called party in the originating message.
Location	C	Include, when the terminating call is answered, the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**
BearerCapability	C	Include, when known (or presumed), to indicate the granted bearer service.

- Table 7-3 defines the parameters of the CCClose message.

Table 7-3 CCClose Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CCCIdentity	M	Identifies the CCC(s)/PDC(s) used to deliver a particular call leg (for example, a trunk identity, a telephone number, or a data networking address).

- Table 7-4 defines the parameters of the CCOpen message.

Table 7-4 CCOpen Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
Content Type – One of: CallIdentity or PDUType	M	**CallIdentity** – Include for circuit-mode calls to identify a particular circuit-mode call instance for the CCC. A unique call identity may be generated for the CCOpen message which is used to correlate other messages with the delivered call content. **PDUType** – Include for packet-mode calls to identify the type of packet data units being intercepted (for example, IP, PPP, X.25 LAPB, ISDN D-channel).
CCCIdentity	M	Identifies the CCC(s)/PDC(s) used to deliver a particular call leg (for example, a trunk identity, a telephone number, or a data networking address).

- Table 7-5 defines the parameters of the Change message.

Table 7-5 Change Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
Previous Calls	M	Identifies all of the existing calls to be affected. Any call identity that is mentioned as a previous call identity, but is not mentioned as a

		resulting call identity is released and may be reassigned to other calls.
Resulting Calls	M	Identifies the CallIdentity(ies) and CCCIdentity(ies) in each of the resulting calls. New unique call identities may be generated for the Change message which are ussed to correlate subsequent messages with the delivered call content.

- Connection message (5E15 and later)

  This message, in combination with the ConnectionBreak message, is used to determine the participants in a subject-initiated conference call, attendant conference call, or call waiting deluxe (N-way/3-way) conference call. See Table 7-6 for parameter information.

  This message is not required when the information reported would be redundant with the information reported by other call event messages.

  When the subject rejoins the conference circuit on hold as a single party, the ConnectedParties parameter is populated as the subject. (If the subject rejoins the held conference call with another party, the Change message is sent, instead of CDC Connection message.)

Table 7-6 Connection Message Parameters (5E15 and later)

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Sequence number.
ConnectionInformation One or more of: ConnectedParties NewParties	M	Identifies parties able to communicate in a call.

- ConnectionBreak message (5E15 and later)
  Table 7-7 defines the parameters of the ConnectionBreak message.

Table 7-7 ConnectionBreak Message Parameters (5E15 and later)

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Sequence number.
ConnectionBreakInformation One or more of: RemovedParties RemainingParties DroppedParties	M	Identifies removed or dropped parties Identifies parties removed from a call. Identifies parties remaining in a call. Identifies parties permanently disconnected from a call.

- The Connection Test message is used to verify the connectivity of the CDC. The CDC Using Voiceband Data Transmission feature (99-5E-8318) in the 5E16.2FR1 software release adds two new uses of the Connection Test message: a heart beat message and a login message.

  A heart beat message is a CDC ConnectionTest message of the form:

  - Neither the IAPSystemIdentity nor the CaseIdentity will be sent as part of a heart beat message.
  - Time Stamp set to the current date and time.

- Memo set to "H_BT" + the number of active cases associated with the GR-30 link. Example: "H_BT009" would be the heart beat memo if 9 active cases were assigned to the link. The number of active cases may be preceded by leading zeroes.

The IAP can be provisioned to either not send heart beat messages or to send them after 1-60 minutes of link inactivity. The CB is optionally expected to ACK/NACK a heart beat message (same as all other messages).

A login message is a CDC ConnectionTest message of the form:

- Neither the IAPSystemIdentity nor the CaseIdentity will be sent as part of a login message.
- Time Stamp set to the current date and time.
- Memo set to "V_ID_5E".

The IAP will only send a login message when provisioned with a login ID. The IAP can send the login message automatically upon link initialization or on demand. The CB is optionally expected to ACK/NACK a login message message (same as all other messages).

Table 7-8 defines the parameters of the ConnectionTest message.

Table 7-8 ConnectionTest Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	O	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
Memo	O	Include any information that may be useful for the TSP to communicate to the LEA (for example, the switching module (SM) tested).

- DialedDigitExtraction message (5E15 and later)

DTMF digit monitoring/extraction is performed for all subject-originated only calls, or when the subject is connected to another telecommunications service provider (TSP).

Dialed digit extraction is supported on LDSU Model II and LDSF DSC3 tone decoders only.

Digit collection is applicable only to subject-initiated calls in a talking state.

NOTE: When DTMF tones are monitored, it may not be possible to determine whether the tones were generated by the subject or the associate due to echo return. With 2-wire echo, the far associate's dialing could register in the subject's tone decoder.

NOTE: When a tone decoder is dropped because of the tone decoder threshold, the DialedDigitExtraction message indicates "tone decoder dropped due to load" in the "Digits" field. See Section 2.4 for more information on tone decoders.

Table 7-9 defines the parameters of the DialedDigitExtraction message.

Table 7-9 DialedDigitExtraction Message Parameters (5E15 and later)

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.

CallIdentity	M	Sequence number.
Digits	M	Identifies DTMF-tones transmitted by the intercept subject after the call is cut-through in both directions. This field also specifies the reason for a tone decoder being dropped. "digit surge tone decoder dropped" "tone decoder dropped due to load" "tone decoder dropped" "no tone decoder available"

- NetworkSignal message (5E15 and later)

  Selected signals sent from the switch towards a subject must be reported as CDC NetworkSignal messages. These signals include audible tones and announcements, visual lamps, and text displays. Table 7-10 defines the parameters of the NetworkSignal message.

  As for alerting (ringing) signal, the switch sends "AlertingOff" in the "Other" parameter for ISDN calls. No such notification is sent for analog calls.

  NOTE: BRCS non-call-associated feature control events result in this message being sent with the CallIdentity parameter empty and the TerminalDisplay parameter populated with generalDisplay information.

Table 7-10 NetworkSignal Message Parameters (5E15 and later)

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Identifies the system containing the intercept access function when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Sequence number.
Signal One or more of: AlertingSignal SubjectAudibleSignal TerminalDisplayInfo Other	M	Audio/visual/text signal sensed by the subject. Defines the pitch and cadence of the alerting (ringing) signal. See Section 7.3.4 for parameter encoding. Reports the type of audible tone applied by the switch towards the subject. See Section 7.3.4 for parameter encoding. Reports information displayed by the switch on subject's terminal (called name/number, calling name/number, redirecting name/number, etc.) Reports other tones provided by the switch which have no equivalent in the J-Standard. See Section 7.3.4 for parameter encoding.

- Table 7-11 defines the parameters of the Origination message.

Table 7-11 Origination Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system. A unique call identity may be generated for the Origination message which is used to correlate other messages. An exception is possible when such an attempt is considered part of an on-going call (for example, three-way calling or conference calling for some systems).
CallingPartyIdentity	C	Include, when more specific than the intercept subject identity associated with the CaseIdentity, to identify the originating party.
CalledPartyIdentity	C	Include, when known, to identify the called party. This is not present

		for calls that were partially dialed or could not be completed by the accessing system.
Input	M	Identifies specific user or translation input including when a call is attempted without input (for example, hotline).
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**
TransitCarrierIdentity	C	Include, when the transit network selection is known, to identify the transit carrier.
BearerCapability	C	Include, when known (or presumed), to indicate the granted bearer service.

- Table 7-12 defines the parameters of the Redirection message.

Table 7-12 Redirection Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call within a system.
Redirected-to PartyIdentity	M	Identifies the redirected-to party.
TransitCarrierIdentity	C	Include, when the transit network selection is known, to identify the transit carrier.
BearerCapability	C	Include, when known (or presumed), to indicate the granted bearer service.
SystemIdentity	C	Included when a call to a wireless subscriber is redirected to another TSP and that identity is reasonably available.

- Table 7-13 defines the parameters of the Release message.

Table 7-13 Release Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system. The call identity is released.
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**
SystemIdentity	C	Included when a call to a wireless subscriber is redirected to another TSP and that identity is reasonably available.

- SubjectSignal message (5E15 and later)

  Table 7-14 defines the parameters of the SubjectSignal message.

  NOTE: This message is not required when information reported would be redundant with information reported by other messages (for example, DialedDigitExtraction message).

  NOTE: For a BRCS feature control event, the DialedDigits parameter is not populated since the Input parameter of the Origination message provides the same information. In addition, BRCS non-call-associated feature control events result in this message being sent with the CallIdentity parameter left blank and the FeatureKey parameter being populated.

  NOTE: This message is not sent when a subject invokes a feature via a Scan Point from an analog line.

Table 7-14 SubjectSignal Message Parameters (5E15 and later)

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Sequence number.
Signal One or more of: SwitchHookFlash DialedDigits FeatureKey OtherSignalInformation	M	Identifies the signal/dialing detected from the subject. e.g., "FLASH" Dialed digits. Feature key pressed (e.g.,"KEY1", "HOLD", "CONFERENCE") e.g. "HOME"

Table 7-15 defines the parameters of the TerminationAttempt message.

Table 7-15 TerminationAttempt Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system. A unique call identity is generated for the TerminationAttempt message which is used to correlate other messages. An exception is possible when such an attempt is considered part of an on-going call (for example, call waiting for some systems).
CallingPartyIdentity	M	Identifies the calling party to extent known.
CalledPartyIdentity	C	Include, when more specific than the subject identity associated with the CaseIdentity, to identify the called party.
BearerCapability	C	Include, when known (or presumed), to indicate the granted bearer service.
RedirectedFrom- Information	C	Include when the incoming call has information about previous redirection.

7.3.4 CDC PARAMETER DEFINITIONS

This section defines the CDC parameters used for wireline CALEA only.

AnsweringPartyIdentity

Identifies the answering party or agent, even if it is the same as the called party in the originating message. See PartyIdentity for details.

BearerCapability

Indicates a requested or granted bearer service. This parameter is not applicable to analog subjects. Encoded according to T1.607 Bearer Capability information element starting with Octet 3. Table 7-16 shows the Bearer Capability information element as defined in the T1.607 standard.

Table 7-16 Bearer Capability Information Element

Bits	8	7	6	5	4	3	2	1
Octet 1	0	0	0	0	0	1	0	0
Octet 2	length of Bearer Capability information element							
Octet 3	1	coding standard		information transfer capability				
Octet 4	0/1 ext	transfer mode		information transfer rate				

Table 7-17 defines the Coding Standard (Octet 3, Bits 6 and 7).

Table 7-17 Coding Standard (Octet 3, Bits 6 and 7)

7	6	Coding Standard
0	0	ITU-T standardized Coding
1	0	National standard

Table 7-18 defines the Information Transfer Capability (Octet 3, Bits 1 through 5).

Table 7-18 Information Transfer Capability (Octet 3, Bits 1 through 5)

5	4	3	2	1	Information Transfer Capability
0	0	0	0	0	speech
0	1	0	0	0	unrestricted digital information
0	1	0	0	1	restricted digital information
1	0	0	0	0	3.1-kHZ audio
1	0	0	0	1	7-kHZ audio

Table 7-19 defines the Transfer Mode (Octet 4, Bits 6 and 7).

Table 7-19 Transfer Mode (Octet 4, Bits 6 and 7)

7	6	Transfer Mode
0	0	circuit mode
1	0	packet mode

Table 7-20 defines the Information Transfer Rate (Octet 4, Bits 1 through 5).

Table 7-20 Information Transfer Rate (Octet 4, Bits 1 through 5)

5	4	3	2	1	Information Transfer Rate
0	0	0	0	0	packet mode calls
1	0	0	0	0	64kbps

Octets 5 - 7 are associated with providing user information Layer 1 - 3 protocol. Octets 4 - 7 of the bearer capability are defaulted.

The BearerCapability parameter is populated by the switch with one of the following:

- Speech calls
- 3.1K Audio calls
- Octets 3 through 7 of the T1.607 Bearer Capability Information Element. (Octet 3 contains the coding standard and information transfer capability.)

CallIdentity

Equal to the unique identity of the subject's activation call attempt. It is generated by the switch and is used by both packet-switched calls and circuit-switched calls. Table 7-21 defines the CallIdentity field(s).

Table 7-21 CallIdentity Fields

Fields	MOC	Usage	Size (in bytes)
Sequence- Number	M	Sequence number	1 □ 25
SystemIdentity	O	Include when the system issuing the SequenceNumber is different than the accessing system. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	1 □ 25

CalledPartyIdentity

Identifies the called party. This must contain at least one of the following: Analog line values (DN and port), ISDN circuit-switched line values (DN, appearance ID, and Terminal Equipment Identity), ISDN packet-switched line values (DN), and/or Trunk value (trunk group number, trunk member number). See PartyIdentity for details.

CallingPartyIdentity

Identifies the originating party by DN or port number. See PartyIdentity for details.

CaseIdentity

Identifies the Intercept Subject. Table 7-22 defines the CaseIdentity field(s).

Table 7-22 CaseIdentity Fields

Fields	MOC	Usage	Size (in bytes)
CaseIdentity	M	Case identity (for example, "FBI-12345" or "NYPD-12345")	1 □ 25

CCCIdentity

Identifies the CCC(s) (used for conveying circuit-call content) or PDC(s) (used for conveying packet-call content). The transmission path associated with a subject's call has only 20 bytes of visible string. Table 7-23 defines the CCCIdentity field(s).

NOTE: This parameter is based on the approved version in J-STD-025, not Bellcore GR2973, Issue 1. The Bellcore standard differs from the J-STD-025 standard. Standard J-STD-025 takes precedence.

For PDC CCCIdentity, the socket address is stored as a character string in the form of A.B.C.D:HHHH where A.B.C.D is an IP address with decimal numbers (0-255) and HHHH is the dynamically-generated port with a hex value (0000-FFFF).

For CCC, CCCIdentity, the trunk group and member is stored as a character string in the form of GGGG-MMMM where GGGG is trunk group number and MMMM is the trunk member. Both trunk group and member are stored in decimal values. The CCCIdentity sepCCCpair.sepXmitCCC and sepRecvCCC are the only ones populated for dedicated (circuit switched) CCCs.

NOTE: For CCC Dial Out feature in the 5E16.2 Software Release, more choices are available. However, the new format is ABBBBB where A is 0 for transmit (sepCCCpair.sepXmitCCC, indXmitCCC), 1 for receive (sepCCCpair.sepRecCCC, indRecCCC), or 2 for combined (combCCC) and BBBBB (a unique number with leading zeros).

Table 7-23 CCCIdentity Fields

Fields	MOC	Usage	Size (in bytes)
combCCC	M	Combined CCC	1 □ 20
sepCCCpair	M	Separated CCC, comprised of sepXmitCCC and sepRecvCCC.	
sepXmitCCC	M	Transmit path from the intercept subject or redirected-to party (trunk group and member number) (source socket address only)	1 □ 20
sepRecvCCC	M	Transmit path from the associate party to the intercept subject (trunk group and member number) (source socket address only)	1 □ 20
indXmitCCC	M	Individual transmit path from the intercept subject or redirected-to party.	1 □ 20
indRecvCCC	M	Individual transmit path from the associate party.	1 □ 20
indCCC	M	Individual CCC without a specified direction. **Used only in CCClose messages.**	1 □ 20

CommunicatingIdentity

Identifies the parties participating in the communication. Table 7-24 defines the CommunicatingIdentity field(s).

Table 7-24 CommunicatingIdentity Fields

Fields	MOC	Usage	Size
CallIdentity	O	Identifies the communicating call identities.	1
PartyIdentity	O	Identifies the communicating call identities.	1-6 times total

			size of PartyID
CCCIdentity	O	Included when content of the resulting call is delivered (to identify the associated CCCs).	

ConnectionInformation

Identifies the parties participating in a call under surveillance. Table 7-25 defines the ConnectionInformation field(s).

Table 7-25 ConnectionInformation Fields

Fields	MOC	Usage	Size
connectedParties	O	Identifies parties able to communicate to each other in a call.	1-6 times total size of PartyID
newParties	O	Identifies one or more parties added to a call.	1-6 times total size of PartyID

ConnectionBreakInformation

Identifies the parties removed from a call under surveillance. Table 7-26 defines the ConnectionBreakInformation field(s).

Table 7-26 ConnectionBreakInformation Fields

Fields	MOC	Usage	Size (in bytes)
removedParties	O	Identifies parties removed from a call (placed on hold).	1-6 times total size of PartyID
remainingParties	O	Identifies parties remaining on a call.	1-6 times total size of PartyID
droppedParties	O	Identifies parties permanently disconnected from a call.	1 times total size of PartyID

Digits

Identifies digits dialed by subject. Table 7-27 defines the Digits field(s).

Table 7-27 Digits Fields

Fields	MOC	Usage	Size (in bytes)
digits	O	String of digits dialed (e.g., "1234", "*123", "#345) or error message specifying the reason for a tone decoder being dropped: "**digit surge tone decoder dropped**" "**tone decoder dropped due to load**" "**tone decoder dropped**" "**no tone decoder available**"	1 □ 32

IAPSystemIdentity

Identifies the system of the Interface Access Point (not the specific location of the subject). IAPSystemIdentity parameter is 1-15 bytes.

Input

Identifies specific user input or translation input (switch capability-based expansion of user input); (for example, speed dialing) including when a call is attempted without input (for example, hotline).

PartyIdentity

Identifies a party to call or call attempt. One or more of the following may be sent. Table 7-28 defines the PartyIdentity field(s).

Table 7-28 PartyIdentity Fields

Fields	MOC	Usage	Size (in bytes)
esn	O	AMPS-based electronic serial number (in hexadecimal, for example, "82ABCDEF"). **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	8
imei	O	GSM-based international mobile equipment identity. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	1 □ 15
tei	O	ISDN-based terminal equipment identity	1 □ 15
spid	O	ISDN-based service profile identifier	3 □ 20
imsi	O	International mobile station identity. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	1 □ 15
min	O	AMPS-based mobile identification number. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	10
dn	O	Called directory number or network-provided calling number (National numbering plan □ up to 10 digits; International □ up to 15 digits; Private Numbering Plan □ up to 15 digits). If more than 15 digits, then the DN will be found in the "content" field of this parameter.	1 □ 15
userProvided	O	User-provided calling number. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	1 □ 15
appearanceID	O	Included for instruments or services with multiple line station, or call appearances. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	1 □ 15
callingCardNum	O	Calling card number. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	1 □ 20
idAddress	O	IP address in decimal quad notation (123.123.123.123) (not a URL). **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	1 □ 32
x121	O	Begin with DNIC	1 □ 15
trunkID	O	Indicates the trunk group, trunk member number, or both, used to identify an associate when other identifying information is not available. This may also identify a subject's agent (for example, screening service).	1 □ 32
subaddress	O	Octet string encoded according to T1.607 Subaddress information element starting with octet 3. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	2 □ 14
genericAddress	O	Indicates use of the generic address.	1 □ 32
genericDigits	O	Indicates use of the generic digits. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	1 □ 32
genericName	O	Indicates use of the generic name. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	1 □ 48
port	O	Identifies a particular equipment port used to identify an associate when other identifying information is not available.	1 □ 32
content	O	Used when none of the other identities are known or to identify the content and special considerations of the supplied identifier(s), especially when the identifier(s) is/are abnormal (for example, international, private, restricted, operator, no address, hotel/motel, coin, etc.).	1 □ 64
isdnHighLayer	O	Included, if known, encoded according to T1.607 High Layer Compatibility information element starting with octet 3. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	2 □ 14
isdnLowLayer	O	Included, if known, encoded according to T1.607 Low Layer Compatibility information element starting with octet 3. **NOT SUPPORTED IN WIRELINE IMPLEMENTATION.**	2 □ 14

PDUType

Indicates the intercepted packet type on a PDC. It is encoded as short, therefore PDUType is 1 byte in length (1 octet is sent to the LEA). Table 7-29 defines the PDUType field(s).

Table 7-29 PDUType Fields

Packet Type (one of the following)	MOC	Usage	Value
isdnBchannel	M	see BearerCapability parameter	00000000
isdnDchannel	M	Intermixed Q.931, Q.932, and X.25	00000001
ip	M	internet protocol packets	00000010
ppp	M	internet point-to-point packets	00000011
x25	M	X.25 LAPB packets	00000100

RedirectedFromInformation

Reports information about the last redirecting party and the original redirecting party on calls that are redirected to the subject. Table 7-30 defines the RedirectedFromInformation field(s).

Table 7-30 RedirectedFromInformation Fields

Fields	MOC	Usage	Size (in bytes)
lastRedirecting	O	PartyIdentity (if known)	See Note
originalCalled	O	PartyIdentity (if known)	See Note
numRedirections	O	Number of redirections, if known.	1 -3
Note: Refer to PartyIdentity for field sizes.			

ReleaseParty

Sent whenever a call or call attempt has ended and all connections associated with the subject or its services have been released.

Signal (AlertingSignal)

Defines the pitch and cadence of the alerting (ringing) signal. Table 7-31 lists the AlertingSignals as defined in the J-Standard.

Table 7-31 AlertingSignals

J-Standard Signal	Comments
AlertingPattern0	Alerting ring pattern for 2-wire line, POTS "Regular Ringing" (2sec on □ 2sec off), Half of 4PSS parties, Half of 8PSS parties, MDN pattern of A, DR pattern of A
	Distinctive alerting-intergroup, alerting ring patterns for 2-wire line (1.6 sec on □ .4 sec off), DR Pattern P (Autovon Precedence and Preemption)
	Alerting ring pattern for 4-wire line (offhook), Routine, Priority (DR pattern F)
	ISDN Alerting Pattern 0, normal alerting (Custom and National ISDN)
AlertingPattern1	Distinctive alerting-intergroup, alerting ring patterns for 2-wire line, Revertive party call for: Half of 4PSS parties (FCFP_SR2,ST2), Half of 8PSS parties (FCEP_RP2,RN2,TP2,TN2), (.5sec on □ 2.5sec off)
	Alerting ring pattern for 4-wire line (350ms offhook, 350ms onhook, offhook), Priority (DR Pattern F)
	Distinctive alerting-intergroup, Alerting ring patterns for 2-wire line (2 pings), MDN pattern B and DR pattern B
	ISDN Alerting Pattern 1, distinctive alerting-intergroup (Custom and National ISDN)
	ISDN Alerting Pattern 6 (Custom ISDN only)
AlertingPattern2	Distinctive alerting-intergroup, Alerting ring patterns for 2-wire line (3 pings), MDN pattern B and DR pattern B
	Alerting ring pattern for 4-wire line (Continuous 1650ms offhook, 350ms onhook), Priority (DR Pattern F)
	Distinctive Alerting □ Special/Priority (1sec on □ 3sec off), 911 ringback for: 2party ONI, ringback both parties, 4pss/8pss, 5party MFR, ringback all
	ISDN Alerting Pattern 2, distinctive alerting - special/priority (Custom and national ISDN)
	ISDN Alerting Pattern 5 (Custom ISDN only)
AlertingPattern3	Alerting ring patterns for 4-wire lines (Continuous 2sec offhook, 4sec onhook), DR pattern E
	Distinctive alerting-intergroup, alerting ring patterns for 2-wire line (1 sec on □ 1 sec off, 1 sec on □ 3 sec off), DR pattern D,

	MFRI B,C,D distinctive, Half of 4PSS parties (FCFP_SR2,ST2), Half of 8PSS parties (FCEP_RP2,RN2,TP2,TN2)
	Distinctive alerting-intergroup, alerting ring patterns for 2-wire line (.3 sec on □ .2 sec off, 1 sec on □ .2 sec of, .3 sec on □ 4 sec off) MDN pattern E and DR pattern G
	ISDN Alerting Pattern 3, EKTS intercom (Custom and national ISDN)
	ISDN Alerting Pattern 7 (Custom ISDN only)
AlertingPattern4	Reminder ring □ ping- ring (100ms on), Call forward ping-ring, also call screening of MSS
	ISDN Alerting Pattern 4 reminder ring (Custom and National ISDN)
callWaitingPattern1	Basic callwaiting tone (300ms burst □ 300ms 440Hz)
	Basic callwaiting tone (380ms burst which adds: 80ms 2130Hz+2750Hz), CallerID on CWT version of CWTON
	ISDN call waiting tone (Custom and National ISDN)
callWaitingPattern2	Incoming Additional Call Tone (300ms burst - 100ms 440Hz □ 100ms Silence □ 100ms 440Hz)
	Incoming additional call tone (380ms burst which adds: 80ms 2130Hz+2750Hz), CallerID on CWT version of CWTON2
	ISDN Incoming additional call tone (National ISDN only)
callWaitingPattern3	Priority Additional Call Tone (500ms burst - 100ms 440Hz □ 100ms Silence □ 100ms 440Hz □ 100ms Silence □ 100ms 440Hz)
	Priority additional call tone (580ms burst which adds: 80ms 2130Hz+2750Hz), CIDCW version of CWTON3
	ISDN Priority additional call tone (National ISDN only)
callWaitingPattern4	Distinctive Callwaiting Tone (700ms burst: 100ms 440Hz □ 100ms Silence □ 300ms 440Hz □ 100ms Silence □ 100ms 440Hz)
	Distinctive Callwaiting Tone (780ms burst which adds: 80ms 2130Hz+2750Hz), CIDCW version of CWTON3
bargeInTone	(900ms burst: 900ms 440Hz)
	ISDN Barge-in tone (National ISDN only)

Signal (AudibleSignal)

Reports the type of audible tone applied by the switch towards the subject. Table 7-32 lists the AudibleSignals as defined in the J-Standard.

Table 7-32 AudibleSignals

J-Standard Signal	Comments
dialTone	Infinite steady (steady 350Hz+440Hz)
	Infinite (steady 350Hz+440Hz)
	ISDN Dialtone (Custom and National ISDN)
recallDialTone	Cadence/steady, repeat three cycles of (100ms 350Hz+440Hz □ 100ms Silence), then steady 350Hz+440Hz
	ISDN Recall Dialtone (Custom and National ISDN)
ringbackTone	Includes audible ring Infinite cadence (2000ms - 440Hz+480Hz) (4000ms Silence)
	Infinite cadence (1640ms 440Hz+480Hz □ 360ms Silence)
	ISDN Ringback/audible tone (Custom and National ISDN)
reorderTone	Infinite cadence (250ms 480Hz+620Hz □ 250ms Silence)
	ISDN Network Congestion/reorder tone (Custom and National ISDN)
busyTone	Infinite cadence (500ms 480Hz+620Hz □ 500ms Silence)
	ISDN busy tone (Custom and National ISDN)
	ISDN busy verify tone (Custom ISDN only)
confirmationTone	(500ms burst □ 100ms 350Hz+440Hz □ 100ms Silence), repeat three cycles of this
	ISDN Confirmation Tone (Custom and National ISDN)
expensiveRouteTone	(900ms burst □ 900ms 440Hz)
	ISDN Expensive route warning tone (Custom and National ISDN)
messageWaitingTone	10 burst dialtone, Cadence/Steady, Repeat 10 cycles of (100 ms 350Hz+440Hz □ 100ms Silence), then steady 350Hz+440Hz
	ISDN Stutter Dialtone (Custom ISDN only)
receiverOffHookTone	Infinite cadence (100ms 1400+2060+2450+2600Hz □ 100m Silence)
	Infinite Steady (Steady 350Hz + 480Hz)
	ISDN off-hook warning tone (Custom ISDN only)
answerTone	ISDN answer tone (Custom ISDN only)

Signal (Other)

Table 7-33 lists signals provided by the switch which do not have an equivalent in the J-Standard.

Table 7-33 Other Signals

Reported As	Comments
High Tone	Infinite Steady, (Steady 480Hz), 911 caller, Operator ringback coin line, Attendant Call through test, Miscellaneous (when announcement is not available)
Preemption Tone	Infinite Steady (440Hz + 620Hz), Precedence and Preemption
Departure Tone 1	(900ms burst 440 Hz) Used for Party Departure Tone
Departure Tone 2*	(Party Departure Tone)
Departure Tone 3*	(Party Departure Tone)
Precedence Departure Tone	(900ms burst 440 Hz) Used for Precedence and Preemption Departure Tone.
Custom Tone	ISDN Custom Tone (Custom ISDN only)
* The tones are reported for CallWaiting and Departure Tone.	

Signal (TerminalDisplayInfo)

Reports information displayed by the switch on the subject's terminal. Table 7-34 defines the TerminalDisplayInfo Signal field(s).

NOTE: The content of this parameter must be identical to the display content encoded in the Display Text Information Element of the Q.931 INFOrmation message. The format of the display information may vary between Custom ISDN (where Display information is encoded in "codeset 6") and National ISDN (where Display information is encoded in "codeset 5").

Multiple NetworkSignal messages may be sent when multiple INFOrmation messages are needed to report the desired Display information. For example, for National ISDN there can be up to 125 characters sent in the Q.931 message. However, the NetworkSignal message length field limitation is 80 characters. So, 80 characters are sent in the first message and the remaining characters are sent in a subsequent message. Custom ISDN has a 40 character limit in the Q.931 message, so all information can be sent in a single NetworkSignal message.

Table 7-34 TerminalDisplayInfo Signal Fields

Fields	MOC	Usage	Size (in bytes)
generalDisplay	O		1..80
calledNumber	O	digits dialed	1..40
callingNumber	O	phone number of the associate calling the subject	1..40
callingName	O	name of associate calling the subject	1..40
originalCalledNumber	O	number originally called	1..40
lastRedirectingNumber	O	last redirected number	1..40
redirectingName	O	name of redirected party	1..40
redirectingReason	O	reason for redirection	1..40
messageWaitingNotif	O	Message Waiting Indicator (lamp)	1..40

TimeStamp

Identifies the date and time (Generalizedtime) that the call event was detected. Table 7-35 defines the TimeStamp field(s).

Table 7-35 TimeStamp Fields

Fields	MOC	Usage	Size (in bytes)
GeneralizedTime	M	Generalized local switch time, as defined in ITU-T standard X.680, in the format: yyyymmddhhmmss.s	

TransitCarrierIdentity

Identifies an interexchange carrier. Table 7-36 defines the TransitCarrierIdentity field(s).

Table 7-36 TransitCarrierIdentity Fields

Fields	MOC	Usage	Size (in bytes)
TransitCarrier- Identity	O	Includes the carrier access code (if applicable), for example, "123" or "10123" or "1012345" or "9501234" and carrier identification code (PIC) (for circuit calls) or the data network identification code (DNIC) (for packet calls).	3-7

7.4 PDC ENCODING FOR PACKET-MODE SERVICES

Intercepted packet-mode data unit (PDU) communications are delivered to an LEA by following these basic steps: the X.25 call content packets is collected by the X.25 packet handler that is supporting the subject under surveillance, copied, encapsulated into the TCP Packet (TPKT) header, encapsulated into TCP/IP messages, routed to the packet handler assigned to deliver the TCP/IP messages to the Law Enforcement Agency (that is, the delivery PH), then additionally encapsulated into X.25 messages which are sent to the X.25 permanent virtual circuit assigned for delivery. Intercepted PDUs include addressing information to associate the PDU with the parties of communication and are delivered without modification, except for possible re-framing, segmentation, or enveloping required for transport.

GLOSSARY

This section provides acronyms and abbreviations used in this document.

AIU
Access Interface Unit

AP
Attached Processor

ASN.1
Abstract Notation One

AT
Administrative Terminal

BRA
Basic Rate Access

BRI
Basic Rate Interface

CALEA
Communications Assistance for Law Enforcement Act

CCC
Call Content Channel

CDC
Call Data Channel

CIS
Call Interception System

CPE
Customer Premises Equipment

CRW

Customized Report Writer

CSV
Circuit-Switched Voice

CSD
Circuit-Switched Data

DCE
Data Circuit-terminating Equipment

DM
Disconnected Mode

DN
Directory Number

DSCS
Digital Switching System for Communicator Services

DSL
Digital Subscriber Line

DTE
Data Terminating Equipment

EAIU
Extended Access Interface Unit

EN
Equipment Number

FMC
Force Management Center

IAP
Intercept Access Point

ICMP
Internet Control Message Protocol

IP
Internet Protocol

IPv4
Internet Protocol version 4

IPPH
Internal Protocol Protocol Handler

ISDN
Integrated Services Digital Network

ISLU
ISDN Line Unit

ISN
Initial Sequence Number

IRS
Initial Receive Sequence Number

ISS
Initial Send Sequence Number

ITU
International Telecommunications Union

LAPB
Link Access Procedures - Balanced

LCKLN
Line Circuit Line Number

LEA
Law Enforcement Agency

MCT
Maximum Combined Throughput

MS
Monitoring Station

MTU
Maximum Transmission Unit

OAP
OSPS Administrative Processor

OSC
Operator Service Center

OSDS
Operating System for Distributed Systems

OSI
Open Systems Interconnection

OSPS
Operator Services Position System

PDC
Packet Data Channel

PDU
Packet-Mode Data Unit

PH
Packet Handler

POTS
Plain Old Telephone Service

PPB
Permanent Packet B-Channel

PSD
Packet-Switched Data

PSTN
Public Switch Telephone Network

PSU
Packet Switching Unit

PVC
Permanent Virtual Circuit

RC/V
Recent Change/Verify

RAIU
Remote Access Interface Unit

RIP
Routing Information Protocol

RISLU
Remote ISDN Line Unit

RNR
Receiver Not Ready

RTAC
Regional Technical Assistance Center

SABM
Set Asynchronous Balanced Mode

SAI
Surveillance Administration Interface

SAS
Surveillance Administration System

SCCS
Switching Control Center System

SM
Switching Module

SMP
Switching Module Processor

SU
Software Update

SVC
Switch Virtual Circuit

TCB
Transmission Control Block

TCP
Transmission Control Protocol

TIA
Telecommunications Industry Association

TPDU
Transport Protocol Data Unit

TPKT
TCP Packet

UA
Unnumbered Acknowledgement

XAT
X.25 Access over a T1 facility

List of Figures

List of Tables

