1. INTRODUCTION

1.1 PURPOSE

This information product provides procedures for the provisioning, maintenance, and troubleshooting of the *5ESS*® switch for the Communications Assistance for Law Enforcement Act (CALEA) application for wireline subscribers only.

NOTE: Regarding network provisioning, it is the responsibility of the switch owner to select the most appropriate network configuration. **Any IP addresses found in this information product are only examples, and any similarities between the examples contained herein and IP addresses used by any telephone company are purely coincidental.**

This information product is intended for those responsible for normal maintenance and network administration of the *5ESS*® switch for wireline subscribers.

For detailed setup information and procedures on the wireless CALEA application, refer to 401-610-615, "*Flexent*®/ *AUTOPLEX*® Wireless Networks Lawfully Authorized Electronic Surveillance (LAES) for CALEA Implementation Guide". A high-level view of how the *5ESS*® switch is used for the wireless CALEA application is provided in 235-200-100, "*Flexent*®/ *AUTOPLEX*® Wireless Networks Applications OA&M Manual".

1.2 UPDATE INFORMATION

1.2.1 REASON FOR UPDATE

This information product has been updated with changes related to IMR 778884. A note Note has been added in Chapter 3, Section 3.8.4 , CDC/PDC IP ADDRESS PROVISIONING, to clarify the appropriate value for the QUALIFIER 3 field on RC view 33.1.

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) SYSTEM CONFIGURATION

(3) FACILITIES PROVISIONING

- (a) SECURED FEATURE ENABLING
- (b) IO PORT GROWTH/DEGROWTH
- (c) AUTHORITY CLASS ASSIGNMENT
- (d) SECURITY ADMINISTRATOR LOGIN AND PASSWORD ADMINISTRATION
- (e) CDC/PDC PROVISIONING
- (f) CCC PROVISIONING

(4) NETWORK TROUBLESHOOTING

(5) MAINTENANCE

(6) INPUT AND OUTPUT MESSAGES

(7) RECENT CHANGE VIEWS - CLASS 33

(8) 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 **comments@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, contact your local Lucent Technologies Account Representative.

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 Lucent Technologies.

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
- **1-317-322-6416** 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 Lucent Technologies *5ESS®* Switch documents that are referenced in this document.

- 235-105-231, *Hardware Change Procedures - Growth*
- 235-105-331, *Hardware Change Procedures - Degrowth*
- 235-105-510, *3B21D Computer Hardware Reference Manual*
- 235-118-251, *Recent Change Procedures*
- 235-118-255, *Recent Change Reference*
- 235-120-010, *CDX Reference Guide*
- 235-120-120, *VCDX User's Guide*
- 235-190-104, *ISDN Feature Descriptions*
- 235-200-100, *Flexent®/ AUTOPLEX® Wireless Networks Applications OA&M Manual*
- 235-600-314, *ECD/SG Data Base Manual*
- 235-600-700, *Input Messages*
- 235-600-750, *Output Messages*
- 401-610-615, *Flexent®/ AUTOPLEX® Wireless Networks Lawfully Authorized Electronic Surveillance (LAES) for CALEA Implementation Guide*

2. SYSTEM CONFIGURATION

2.1 OVERVIEW

In the 5E14 software release, Lucent Technologies' solution to government-mandated lawfully-authorized electronic surveillance is a three-feature set (CALEA TCP/IP DSL Access, 99-5E-4908; TCP/IP Suite Functionality, 99-5E-4907; and CALEA-Core, 99-5E-4275 [SFID 509 for non-U.S. North American Region telephone service providers]) providing Access, Delivery, and Administration functionality. The Access and Delivery functions are internal to the *5ESS*® switch.

The 5E15 software release contains feature 99-5E-7599, CALEA Punch List (the second phase of Lucent's CALEA application). This feature provides compliance with the additional requirements mandated by the government via the J-STD-025A ballot copy. There is no SFID associated with this feature.

The 5E15 software release also contains feature 99-5E-8199, TCP/IP Security Enhancement for CALEA. This is a secured feature. The Security Feature ID (SFID) needs to be turned on to activate the feature. In addition, the Optional Feature ID (OFID) is also provided to allow the feature to be turned on or off. This feature enhances the switch's ability to thwart or slow down various IP (internet protocol) attacks that would affect the stability of performance of the SMPs (switching module processor) and PHs (packet handlers) involved in the CALEA TCP/IP traffic.

The 5E16.2 software release contains the enhancement feature, 99-5E-8221, Dial Out CDC and CCC Enhancement to CALEA-core (SFID 509) and CALEA Punchlist. This enhancement uses dial out CDC and CCC connections 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 facility 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 a local LEA with POTS or ISDN termination. 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 will support combined, separated, mixed CCC transmit, and received delivery modes.

The 5E16.2 FR1 software release contains the CALEA CDC with Voice Band Data Transmission feature (99-5E-8318). It 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.

The Administration function is a Surveillance Administration terminal and ROP connected directly to the administrative module (AM).

The access function intercepts a subject's communication and reports Call Progress Data and Call Content to law enforcement. Surveillance delivery capabilities are responsible for transporting call content and/or call progress data from the subject's switch to law enforcement monitoring sites. Surveillance information is sent to the law enforcement agency (LEA) by sending CDC messages and PDC packets in TCP/IP messages over X.25 permanent virtual circuits (BRI or T1). Call content itself is delivered over Call Content Channels (CCCs) (T1 trunks) from the subject's switch or Intercept Access Point (IAP) to the LEA. Alternatively, the CDC with Voice Band Data Transmission feature (99-5E-8318) allows CDC messages to be sent to an LEA

over analog line interfaces.

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

The BRI and the T1 (XAT) interfaces are supported on the SM, SM-2000, Extended Switch Module 2000 (EXM-2000), RSM, Optical Remote Module (ORM), or Distant Remote Module 2000 (DRM-2000). The BRI and the T1 (XAT) interfaces are supported on either a PSU1 or PSU2, and on either a PI1 or PI2. The BRI and the T1 (XAT) interfaces are supported on either a DF-1, DF-2, or DFMP.

The BRI is supported with the PH3 or PH4, and with the ISLU1, ISLU2, RISLU, TR-303 on IDCU, TR303 on DNU-S, AIU, or EAIU.

The T1 (XAT) is supported with the PH3 or PH4. The T1 is supported with a DFI-XT, DFI-2XT, or DNU-S.

The BRI supports permanent virtual circuit packet mode delivery service on either the B1 channel, the B2 channel, or both.

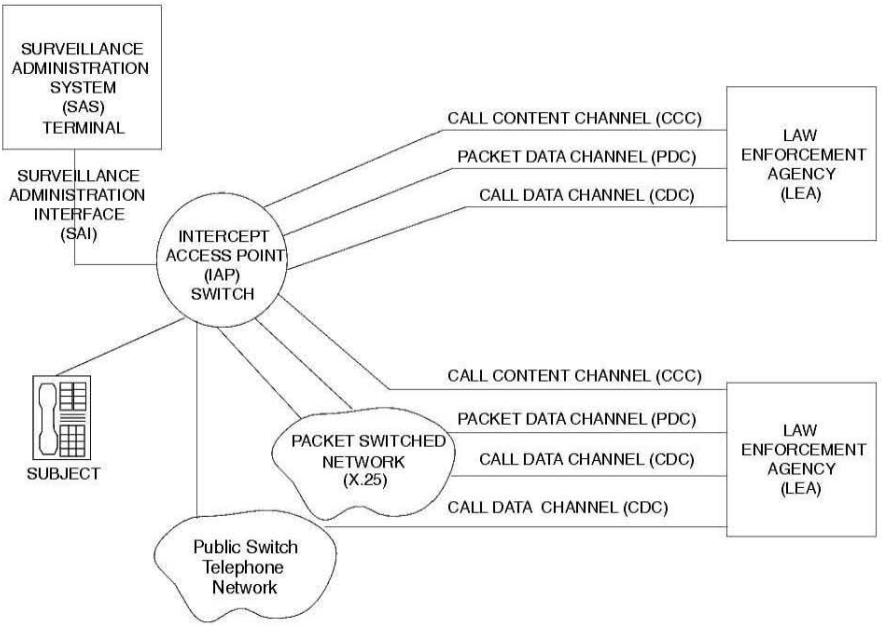
The surveillance administration capability activates, maintains, and deactivates surveillance within a service provider network. The surveillance administration operations system interface is based on a human machine language over an ASCII terminal interface and a restricted Recent Change menu interface in the 5E14 software release. This restricted interface will only have access to the CALEA-specific views. General RC menus will not be available.

Beginning with the 5E15 software release, the CALEA Punchlist feature makes available the capability for the surveillance administrator to have full access (read, update, delete, insert) to all Recent Change classes and views. This capability is controlled by the new **ADMIN ACCESS** field on Recent Change view 8.1. Switch maintenance personnel must set the **ADMIN ACCESS** field to **Y** and notify the Surveillance Administrator that this action has been taken. The default value for the **ADMIN ACCESS** is **N**.

The SAS interface to the *5ESS*® switch CALEA data is restricted by password and authority class to prevent casual access to surveillance data by office technicians. There is a need for office technicians to maintain the switch data. Office Data Base Editor (ODBE) is a tool which normally allows unrestricted access to the switch data for correcting data corruption problems. For the CALEA feature set, the global parameter GLCALIPADR is viewable, but has been blocked from ODBE update. Any attempt to change GLCALIPADR via ODBE will result in the response:
You are not allowed to update this office parameter using ODBE.

Figure 2-1 provides an overview of the CALEA network, including the SAS terminal (which interfaces directly with the switch), the intercept access point switch (the *5ESS*® switch), the LEA collection facility interfaces, and the interfaces (CCC, CDC, PDC) between the switch and the LEAs.

The channels may be provisioned directly to the law enforcement collection facility, or routed though a transmission network compatible with 64KBps clear-channel service. Tandem switching of the CCCs is not possible.



CALEA NETWORK

Figure 2-1 CALEA Network Overview

2.2 SYSTEM ARCHITECTURAL CONSTRAINTS AND IMPACTS

This feature set requires no hardware changes and no significant software changes of a system architecture nature. Two TTYs must be provisioned for surveillance administration use (input and output), but the hardware itself is not new or different.

The following chart lists the items needed for the CALEA application in the central office.

Equipment	Parts Needed
XAT	An 8-pin straight-thru RJ-45 cable between D4 channel bank and DSU/CSU. DSU/CSU that extracts the DSx from the XAT (X.25 Across T1). V.35 cable between the DSU/CSU and the router
DSL BRI	An 8-pin straight-thru RJ-45 cable between the router's BRI port and ANSI (2B1Q) NT1U device. An ANSI (2B1Q) NT1U device.

	An 8-pin straight-thru RJ-45 cable between the NT1U and the 353a power supply. A 353a power supply. An 8-pin straight-thru RJ-45 cable between the 353a power supply and the patch panel.
SAS RC Terminal	250 foot IOP to DB25 Cable from AM backplane to SAS RC Terminal. Dummy Terminal with keyboard and power cord. 4800 E-7-1 settings on Dummy Terminal.
SAS ROP Terminal	250 foot IOP to DB25 Cable from AM backplane to SAS ROP Terminal. Dummy Terminal with keyboard and power cord. 9600 E-7-1 settings on Dummy Terminal.
ROP	* Already exists in Central Office. 1200 E-7-1 settings on Terminal.
STLWS	* Already exists in Central Office. 9600 E-7-1 settings on Terminal.
CCC Trunk	T1

2.3 OPERATIONS SYSTEMS IMPACTS

No standard switch administrative operations systems will be impacted by this feature, however, OS applications not specifically intended for CALEA access will not be able to access CALEA data.

2.4 SYSTEM COMPONENTS

2.4.1 EXTERNAL SYSTEM FUNCTIONALITIES

The external system (*5ESS*® switch, SAS and LEA monitor boxes) will perform the following tasks:

- provide user interfaces to identify, provision and activate surveillances for Circuit and Packet calls,
- provision TCP/IP and associated delivery facilities (PVCs on X.25 BRIs and/or T1 (XAT) trunks),
- call content storage, retrieval and distribution,
- call associated data storage and distribution, and
- multiple agents (organizations) handling.

2.4.2 INTERFACES BETWEEN EXTERNAL SYSTEMS AND THE SWITCH

There are four interfaces from the *5ESS*® switch to the external systems:

- IO Port Interface

  The SAS terminal has at least two connections to the switch via IO port(s) in the AM to send MML input commands, receive output reports and use RC/V menu/text. The MML commands, RC/V interface and reports are associated with provisioning surveillances and activation/deactivation of the CALEA feature.

Although it is not recommended, a service provider can reuse the existing TLWS or RC/V (but not MCC or SCC) terminal to perform the CALEA SAS functionalities.

- Circuit Call Content Trunk Interface

  Circuit Call Content will be delivered via digital private facility (PF) outgoing trunks using no signaling and having a UCD hunt type. The CCC trunks are supported with a DFI-XT, DFI-2XT, DNU-S, or OIU. A minimum of two trunks are used for each call per Level 2 surveillance case. A single surveillance may use up to 30 CCC pairs - 60 trunks total. Each subject DN may be monitored by up to 5 LEAs. See Figure 2-3 for an overview of the CCC trunks within the CALEA network.

  NOTE: In reference to Figure 2-3 , keep these things in mind:

  - An STSX-1 will **never** go directly to an LEA collection facility.
  - SM2000 is ideal for a high capacity of surveillances.

  When assigning a trunk, the new status field has three possible values: NULL, CRES (C-tone-reserved) and CTONE (C-tone-applied). NULL indicates that the trunk is not for CALEA use. CRES indicates that the trunk is for CALEA use but not currently assigned to a surveillance and CTONE indicates that the trunk is assigned to a CALEA surveillance. When CCC trunks are assigned to a surveillance, the Surveillance Administrator sets CTONE to either HIGHTONE or NULL, based on the LEA's requirements. C-Tone indicates that the trunk is active, assigned to a surveillance case, and not currently supplying call content. Note that a trunk member that has CALEA status of CTONE cannot be deleted.

- Socket X.224 TCP/IP Interface

  The call-associated data for circuit and packet calls will be delivered via the Socket TCP/IP interface and encapsulated using X.224 (provides a header containing the length of the stream of bytes associated with a message).

- GR-30 CDC Interface

  An analog line termination can be used to establish a CDC connection to an LEA. This GR-30 CDC interface will send ASN.1 encoded CDC messages using Frequency Shift Key (FSK) signaling at 1200 bits per second.

See Figure 2-2 for an overview of the CALEA network.

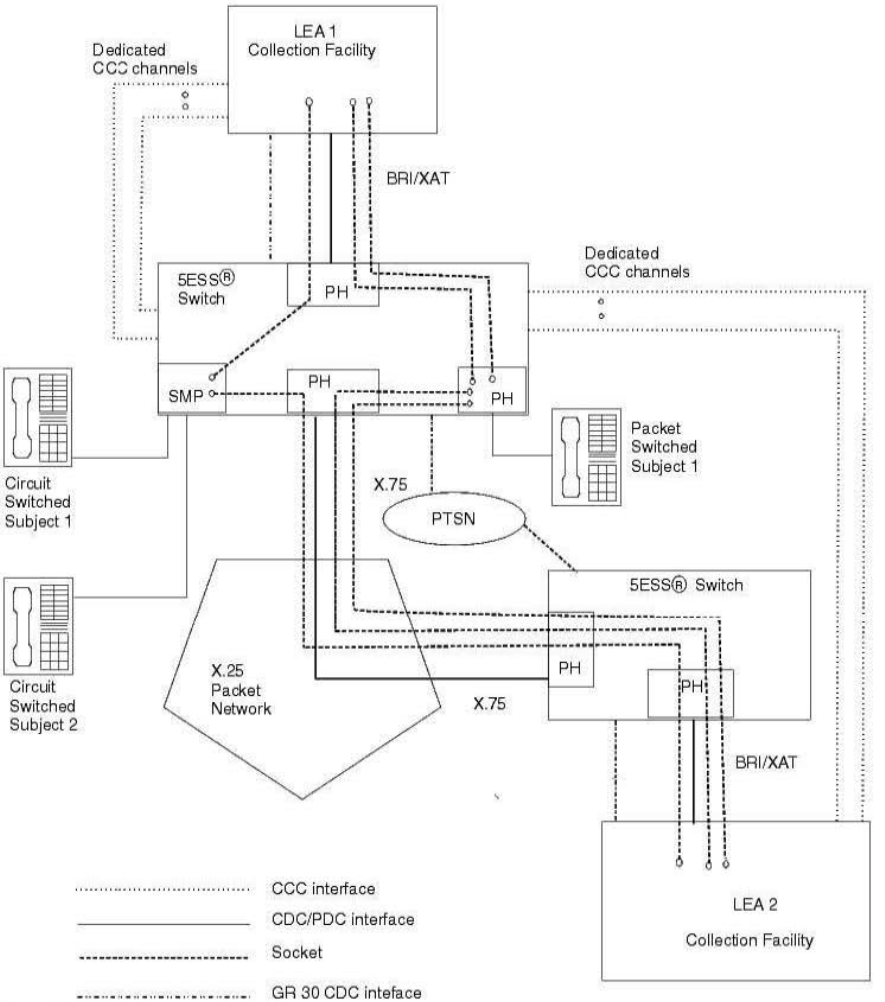


Figure 2-2 CALEA Network Diagram

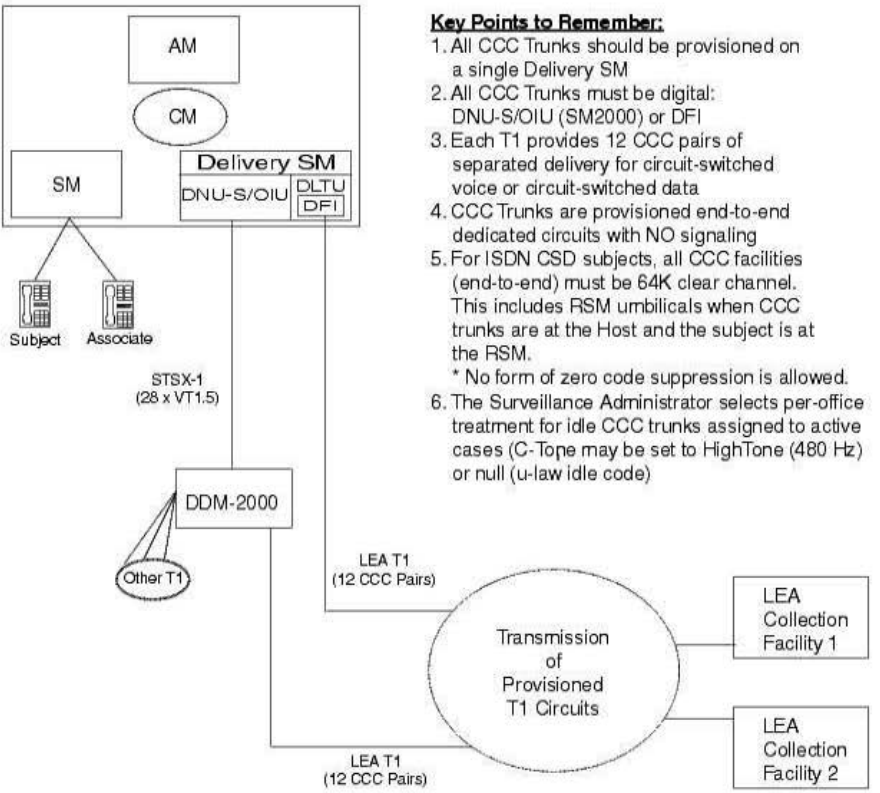


Figure 2-3 CCC Quick Reference

2.5 TONE DECODERS (5E15 and later)

2.5.1 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.

2.5.2 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 5ESS 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.

2.5.3 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 to 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.

Refer to Chapter 4 for information on tone decoder error and corrective actions.

2.5.3.1 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.

2.5.3.2 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.

2.5.4 PROVISIONING ADDITIONAL TONE DECODERS

Depending on the number of surveillances and the number of tone decoders used, additional tone decoders may need to be provisioned for the office.

See 235-070-100, *5ESS Switch Administration and Engineering Guidelines*, for information on adding tone decoders to SMs and SM-2000s.

NOTE: Model 1 DSU on an SM does not support the CALEA Punchlist feature. Model 1 DSU can be upgraded to Model 2 DSU (with TN1637). Model 2 (with TN1637, TN833, or TN1890) DSU or newer model can support the CALEA Punchlist feature in the 5E15 software release.

3. FACILITIES PROVISIONING

3.1 FACILITIES OVERVIEW

Figure 3-1 gives an overview of the switch administrator's required tasks when preparing the switch for use of the CALEA feature set. These tasks are performed via the Recent Change terminal.

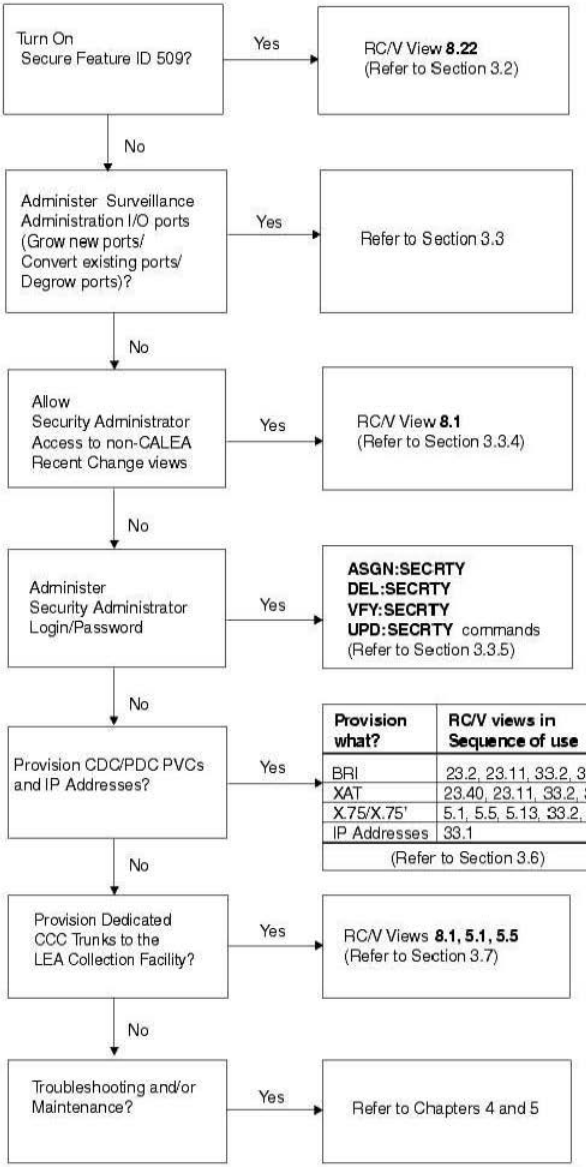


Figure 3-1 Switch Administration Task Overview

3.1.1 SAS INTERFACE

The Surveillance Administration System (SAS) interface is simply a password-protected RC/V terminal, connected to the switch via a TTY port. If strong authentication and encryption capabilities are desired, external equipment must be supplied by the telephone company in accordance with local security practices. Provisioning a dedicated CALEA TTY follows existing procedures.

3.1.2 TRUNKS AND DATA LINKS

The provisioning of surveillance trunks and data links is done using the standard switch maintenance capabilities of the *5ESS*® switch. The trunks and data links needed for surveillance will be the usual equipment found in the *5ESS*® switch with no special requirements. The number of lines provisioned between the switch and the LEA collection facility is beyond the scope of this document. Each service provider should know the average number of surveillances occurring on each of its switches and provision accordingly.

NOTE: There is no Talk/Monitor or TLWS access to CCCs assigned to a case.

3.1.3 IP ADDRESSES

Provisioning of IP Addresses is required for all SMPs. The provisioning of the PHs should be limited to the PH(s) designated as delivery PHs for CDC (Call Data Channel). When PDC (Packet Data Channel) is used, the PH the subject resides on and ISM PHs from the subject's SM to the SM that the delivery PH resides on should also be provisioned.

- Put the *5ESS*® switch intranet behind a Gateway Router/Firewall so that local IP addresses can be used on the switch, but the LEA can use internationally registered IP addresses obtained from the Network Information Center (NIC) if they choose. (Class A and/or Class B)

- Agree with the LEA to use local IP addresses only, however the LEA will require a Gateway Router if they wish to attach their nodes to the internet.

NOTE: The customer should not configure their switch with duplicated IP addresses or connect to LEA collection boxes with identical IP addresses. In the same token, neither should the LEA collection boxes connect to switches with duplicate IP addresses.

It is the responsibility of the switch owner to select the most appropriate network configuration. **Any IP addresses found in this information product are only examples, and any similarities between the examples contained herein and IP addresses used by any Service Provider are purely coincidental.**

3.2 SECURED FEATURE ENABLING

This section contains the procedure for enabling the 5E14 CALEA-Core secured feature (99-5E-4275).

NOTE: The enabling of SFID 509 is not required for telephone service providers (TSPs) in the 50 United States and U.S. territories. The CALEA feature is automatically enabled, by Lucent Technologies, for these NAR TSPs. A telephone service provider in any other country in the North American Region (for example, Canada) operating a *5ESS*® switch and wanting to use the CALEA

functionality, must perform this enabling procedure.

3.2.1 PURPOSE

Secured Feature (SFID) 509 must be turned on via Recent Change view 8.22 (routine switch personnel responsibility) prior to the feature being activated via RC view C.1 (Security Administrator responsibility). If the SFID is not turned on, the CALEA feature can **not** be activated. However, the CALEA feature may be inactive, although the SFID is turned on.

3.2.2 PLANNING

This is a one-time task (unless the SFID is disabled for some reason). The PASSWD and MAP LIST information must be obtained from the Lucent Technologies Customer Account Team.

3.2.3 REQUIRED CONDITIONS

The switch must be running a 5E14 software release with the CALEA-Core feature software.

3.2.4 REQUIRED TOOLS

A non-CALEA Recent Change terminal is required for accessing the general Recent Change database.

3.2.5 PROCEDURE

(1) Via RC/V terminal, access view 8.22, SECURED FEATURE UPGRADE, and populate the following fields:

FIELD	VALUES
FEATURE ID	0
MODULE	OFC
PASSWD	(Obtain from Lucent Technologies SFID Administrator)
MAP LIST	(Obtain from Lucent Technologies SFID Administrator)

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.3 SECURED FEATURE ENHANCEMENTS

3.3.1 TCP/IP Security Enhancement for CALEA (99-5E-8199)

This feature (99-5E-8199) provides a set of security measures that are enhancements to the CALEA-CORE feature (99-5E-4275). These security measures are implemented in the *5ESS*® switch, specifically, in the PHs where the X.25 Permanent Virtual Circuits (PVC) are provisioned and terminated for the use of CALEA CDC or PDC. The supported PH images are PH3C, PH4A, and PH4G. These measures are the implementation of rules that take advantage of the unidirectional nature of CALEA TCP/IP messaging. If any violations of the rules are detected, the IP (internet protocol) datagram is ignored. In addition, fault recovery actions are triggered that will operate on the High Level Data Link (HDLC) channel that supports the X.25 PVC. Persistent violations can take the X.25 PVC out of service. While the PVC is out of service the SAS ROP reports may also be observed. This is a secured feature and therefore requires a secured feature identifier (SFID 628). In conjunction with the SFID, this feature requires an optional feature identifier (OFID 708) that will allow the feature to be turned on or off.

Refer to Chapter 3, Section 3.8.9 for activation and deactivation procedures for this feature.

3.4 NON-SECURED FEATURE ENHANCEMENTS

3.4.1 Dial Out CDC and CCC Enhancement for CALEA (99-5E-8221)

This feature provides alternative provisioning as an enhancement to the CALEA core feature (99-5E-4275).

For CDC (Call Data Channel) dial out, the SVC connection will be established to a local LEA facility via a BRI or XAT termination. The SVC can also be established to a remote LEA with BRI or XAT connection over X.75 or X.75' interface through the public X.25 network. The SVC will not be established until CDC data is ready to be sent. The SVC connection may be torn down by the LEA if there is no message to be sent after 60 minutes.

For dial out CCC (Call Content Channel), 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 an SS7 or MF trunk over the public switched telephone network. In both cases, the CCC connection will not be established until the subject call is intercepted by answering the Destination LEA DN(s). The following CCC delivery modes are supported:

- **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.
- **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.

3.4.2 CALEA CDC with Voice Band Data Transmission (99-5E-8318)

This feature is an enhancement to the Dial Out CDC and CCC Enhancement for CALEA feature (99-5E-4275). This enhancement allows service providers to setup a CDC (Call Data Channel) 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.

3.5 SURVEILLANCE ADMINISTRATION SYSTEM (SAS) INTERFACE PROVISIONING

3.5.1 OVERVIEW

The SAS represents the entity sending messages through the Surveillance Administration Interface (SAI) to enable the setup, activation, modification, and deactivation of surveillances. The SAS may be a manual or automated system. For the *5ESS*® switch implementation, the SAS is a terminal which supports both MML commands and Recent Change activity.

SAS Interface provisioning includes

- IO port growth,
- Authority Class assignment, and
- Security Administrator login assignment.

NOTE: The procedures for each of these four provisioning tasks must be performed in the order they appear in this section.

3.5.2 IO PORT GROWTH/DEGROWTH

The *5ESS*® switch supports two AM IOP 9600bps asynchronous ports for the LAES administrative system interface. These two CALEA TTY ports are added via ECD high level form "ttyadd."

The "ttyadd" function provides a high-level interface to the ECD recent change allowing the customer to input minimal data to populate the necessary low-level ECD forms. The "ttyadd" function includes TTY26 (CALEASAS) and TTY27 (CALEAPRT).

NOTE: Although it is not recommended, a service provider can reuse the existing RC/V (but not MCC, SCC, or TLWS) terminal to perform the CALEA SAS functionalities.

The "ttyadd" function is invoked in the same manner for a 3B21D, VCDX and DRM.

Accessing the "ttyadd" form, adding correct data, and starting execution, cause messages to be displayed on the terminal screen. These messages request the provisioner to diagnose, restore, power up, power down, or connect hardware.

The CALEA TTY used by surveillance/security administrators for command input has no message class assigned since manual reports are sent to the terminal where commands are issued. The other CALEA TTY (receive only printer) has security and surveillance spontaneous message classes. Message classes and authority records for SURLEA (used to send output to SAS terminal and SAS ROP) and SECLEA (used to send output to the SAS ROP only) and log file CACMDLOG will be added to the base ECD. Additional low-level ECD updates are required to setup the CALEA authority values.

The TTY port to perform administrative tasks must be set to have the following characteristics:

- MML text only interface (similar to a Recent Change and Verify terminal)
- Dialogue timeout timer in ECD will be set to 0 (no timeout).
- The terminal authority checking shall be provided.
- The assignments of authorities to the CALEA terminal can be executed from an MML command at the site.

The TTY port to receive security and surveillance spontaneous reports will be set to have the following characteristics:

- MML text only interface (similar to ROP)
- Dialogue shell is not available.

- The spontaneous report message classes for both security and surveillance administrators shall be assigned to this device.

There are several possibilities for TTY growth and degrowth, depending on office configuration. In this section are procedures for

- CALEA Input TTY Growth (3B21D)
- CALEA Output TTY Growth (3B21D)
- CALEA TTY Degrowth (3B21D)
- CALEA Input TTY Growth (VCDX or DRM)
- CALEA Output TTY Growth (VCDX or DRM)
- CALEA TTY Degrowth (VCDX or DRM)
- Converting Existing RC/V TTY to CALEA Input TTY (All Platforms)
- Converting Existing RC/V TTY to CALEA Output TTY (All Platforms)
- Converting Existing STLWS TTY to CALEA Input TTY

3.5.2.1 CONVERT EXISTING RC/V TTY TO CALEA TTY

Instead of growing new TTY ports, existing RC/V (but not MCC, TLWS, or SCC) terminals can be converted to CALEA-specific TTYs.

NOTE: Once a surveillance is established, the switch may generate spontaneous reports as a result of surveillance-affecting events. These reports are routed to the CALEA ROP. Therefore, the recommended procedure is to grow dedicated CALEA input and output TTYs.

3.5.2.2 PLANNING

When provisioning dedicated CALEA TTYs, this procedure should be performed in advance of obtaining a court-order. When provisioning an existing TTY for CALEA use, only to reprovision it for normal use again, this procedure is performed whenever a surveillance is ordered and there is no dedicated TTY for lawfully authorized electronic surveillance (LAES) use.

3.5.2.3 REQUIRED CONDITIONS

All prerequisites are covered within each procedure.

3.5.2.3.1 CALEA INPUT TTY GROWTH FOR 3B21D

3.5.2.3.1.1 OVERVIEW

The flexible input/output processor (FIOP) eliminates the need for adding a growth IOP when there is room for the peripheral device in an existing IOP. The FIOP is an efficient, simplified way to add or delete all of the

low-level forms associated with a particular input/output processor (IOP) device.

3.5.2.3.1.2 PROCEDURE

NOTE: This procedure consists of the following subprocedures. Unless otherwise stated, the subprocedures must be performed in the order stated.

3.5.2.3.1.2.1 Identify the Hardware Supporting the CALEA Input TTY Interface.

The following hardware supports the CALEA Input TTY interface:

- Teletypewriter controller (TTYC) number
- Teletypewriter (TTY) number
- IOP number
- PORT number
- Peripheral controller (PC) number.

3.5.2.3.1.2.2 Perform Port Switch

(1) At master control center (MCC), ensure terminal is in CMD mode.

(2) Type and enter **112**

Response: MCC page 112 is displayed.

(3) Is the maintenance cathode ray tube (MCRT) and/or the receive-only printer (ROP) connected to the maintenance teletypewriter peripheral controller (MTTYC) associated with the input/output processor (IOP) that is going to be removed from service?

If **YES**, continue.
If **NO**, go to **3.5.2.3.1.2.3 .**

(4) Set port switches **EQL - PCCA 0: 045-186** to the **AUTO** position if not already in the **AUTO** position.

(5) At MCC, type and enter one of the following to perform the port switch:

- **401** (switches both MCRT and ROP)
- **402** (switches ROP only)
- **403** (switches MCRT only).

(6) At MCC page 112, verify the MCRT and ROP are not connected to the selected IOP.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.1.2.3 Enter *UNIX*® Real Time Reliable (RTR) System Recent Change and Verify (RC/V)

(1) Is master control center (MCC) or RC/V terminal to be used?

MCC proceed to Step 2.

RC/V proceed to Step 8.

(2) At MCC, ensure terminal is in command mode.

(3) At MCC, do Steps 4 through 7.

(4) Type and enter CMD **199**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(5) Type and enter **incore**

Response: Cursor at **2.review only**

(6) Type and enter **n**

Response: Cursor at **3.journaling**

(7) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(8) At RC/V terminal, type and enter **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(9) Type and enter **incore**

Response: Cursor at **2.review only**

(10) Type and enter **n**

Response: Cursor at **3.journaling**

(11) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.1.2.4 Enter High-Level Forms

(1) Type and enter **toggle**

Response: Takes you to the high-level forms.

(2) Type and enter **help**

Response: List of all high-level forms available.

NOTE: While trying to grow the CALEA Input TTY, a prompt to do corrective action before continuing may appear if any of the following states are encountered:

- Attempting to grow the CALEA Input TTY in a slot with a device in the equip state.
- The slot selected has a device in the unequip state.

If any of the previously mentioned states are present, the high-level delete form must be executed. The procedures for deleting existing forms are in 235-105-331, *5ESS® Switch Hardware Change Procedures - Degrowth.*

(3) Type and enter **iopslots**

Response: **iopslots** form displayed.
Cursor at **1. unit_name:**

(4) Type and enter **IOP**

Response: Cursor at **unit_number:**

(5) Type and enter appropriate unit number (**0**, **1**, **2**, or **3**).

Response: List of all IOP slots assigned.

(6) Type and enter **<**

Response: Exit **iopslots** form.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.1.2.5 Insert TTYC Data

NOTE: An **!** may be entered any time prompted to abort the form and return to the state when the form was started.

(1) If there is an existing TTYC, a new TTYC may not have to be grown. Go to **3.5.2.3.1.2.7** .

(2) Type and enter **ttycadd**

Response: **ttycadd** form displayed.
Cursor at **1. ttyc_name:**

(3) Type and enter appropriate TTYC number.

Response: Cursor at **2. packname:**

(4) Type and enter appropriate packname (**tn74** or **un582**).

Response: Cursor at **3. slot:**

(5) Type and enter appropriate slot position.

Response: Cursor at **4. IOP_number:**

(6) Type and enter appropriate IOP number (**0**, **1**, **2** , or **3**).

Response: Cursor at **5. plu_unit_name:**

(7) Type and enter appropriate data or **CARRIAGE RETURN.**

Response: Cursor at **6. plu_unit_number:**

(8) Type and enter appropriate data or **CARRIAGE RETURN.**

(9) Type and enter **i**

(10) The low-level forms will now be added automatically.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.1.2.6 Complete TTYC Hardware Installation

NOTE: Use this procedure along with the prompts on the selected terminal.

(1) ***First prompt:*** **Remove IOP x and power it down. When complete, hit return to continue or ! to abort.**

At selected terminal, type and enter **RMV:IOP=**x**;**

Where: x = IOP number receiving the new device.

Response: **REMOVE IOP** x **COMPLETED**

At the IOP power switch, simultaneously depress the **MOR** and **OFF** switches.

Press **CARRIAGE RETURN.**

(2) ***Second prompt:*** **Install TTYC x - hit return to continue or ! to abort.**

Installation Function

Press **CARRIAGE RETURN.**

(3) ***Third prompt:*** **Power up and restore IOP x. After ATP hit return to continue or ! to abort.**

At the IOP power switch, simultaneously depress the **MOR** and **ON** switches.

At selected terminal, type and enter **RST:IOP=**x**;**

Where: x = IOP number receiving the new device.

Response: **RESTORE IOP** x **COMPLETED**

Press **CARRIAGE RETURN.**

(4) Type and enter **<**

Response: Exit the ttycadd form.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.1.2.7 Insert TTY Data

NOTE: An **!** may be entered any time prompted to abort the form and return to the state when the form was started.

(1) Type and enter **ttyadd**

Response: **ttyadd** form displayed.
Cursor at **1. tty_name:**

(2) ***Note:*** Fields not specified receive the default value by entering **CARRIAGE RETURN.**

Type and enter the following data:

1. tty_name:	enter **TTY26**
2. baud_rate:	enter (as specified or **CARRIAGE RETURN**)
3. login_term:	enter **n**
4. auth_chk:	enter **t**
5. term_type:	enter (as specified or **CARRIAGE RETURN**)
6. line_mode:	enter (as specified or **CARRIAGE RETURN**)
7. port:	enter **0**, **1**, **2**, or **3**
8. ttyc_number:	enter **TTYC** controller number
9. plu_unit_name:	enter (as specified or **CARRIAGE RETURN**)
10. plu_unit_number:	enter (as specified or **CARRIAGE RETURN**)

NOTE: If a UN582 is equipped, you are allowed to use ports 0-3.
If a TN74 is equipped, you can only use ports 2 and 3.

(3) Type and enter **i**

(4) The low-level forms will now be added automatically.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.1.2.8 Complete TTY Hardware Installation

NOTE: Use this procedure along with the prompts on the selected terminal.

(1) ***First prompt:*** **Remove IOP x from service and power down. Hit return to continue or ! to abort.**

At selected terminal, type and enter **RMV:IOP=**x**;**

Where: x = IOP number receiving the new device.

Response: **REMOVE IOP** x **COMPLETED**

At the IOP power switch, simultaneously depress the **MOR** and **OFF** switches.

Press **CARRIAGE RETURN.**

(2) ***Second prompt:*** **Physically connect TTY x. Hit return to continue or ! to abort.**

Installation Function

Press **CARRIAGE RETURN.**

(3) ***Third prompt:*** **Power up and restore IOP x. Hit return to continue or ! to abort.**

At the IOP power switch, simultaneously depress the **MOR** and **ON** switches.

At selected terminal, type and enter **RST:IOP=**x**,UCL;**

Where: x = IOP number receiving the new device.

Response: **RESTORE IOP** x **COMPLETED**

Press **CARRIAGE RETURN.**

(4) ***Fourth prompt:*** **Remove TTYC x from service. Hit return to continue or ! to abort.**

At MCC, type and enter **RMV:TTYC=**x **;**

Where: x = Appropriate controller number.

Response: **RMV TTYC** x **COMPLETED**

Press **CARRIAGE RETURN**.

(5) ***Fifth prompt:*** **Diagnose and restore TTYC x. When complete, hit return to continue or ! to abort.**

NOTE: All tests pass (ATP) must be achieved before continuing.

At MCC, type and enter **DGN:TTYC=**x**,RAW,TLP;**

Where: x = Appropriate controller number.

Response: DGN TTYC ***x*** **COMPLETED ATP**

At MCC, type and enter **RST:TTYC=**x**;**

Where: x = Appropriate controller number.

Response: **RST TTYC** x **COMPLETED**

Press **CARRIAGE RETURN**.

Response: **FORM INSERTED**

(6) Type and enter **<**

Response: Exit the ttyadd form.

(7) Type and enter **toggle**

Response: Low-level form displayed on screen.

(8) Type and enter **trbegin**

Response: 1.tr_name

(9) Enter a carriage return

Response: Enter Execute, Change, Substitute, Validate, or Print:

(10) Type and enter **e**

Response: Enter Form Name:

(11) Type and enter **authdef**

Response: I=Insert R=Review U=Update D=Delete :

(12) Type and enter **u**

Response: 1.comgr_name:

(13) Type and enter **SURLEA**

Response: Enter Update, Change, Substitute, Validate or Print:

(14) Type and enter **c**

Response: Change field:

(15) Type and enter **5**

Response: 5.log_flag

(16) Type and enter **y**

Response: Change field:

(17) Type and enter **8**

Response: 8.log_flag

(18) Type and enter **y**

Response: Change field:

(19) Enter a carriage return

Response: Enter Update, Change, Substitute, Validate or Print:

(20) Type and enter **u**

Response: 1.comgr_name:

(21) Type and enter **SECLEA**

Repeat Steps 15 through 21

(22) Type and enter **RCV**

Repeat Steps 15 through 21

(23) Type and enter **FHADM**

Repeat Steps 15 through 21

(24) Type and enter **<**

Response: Enter Form Name:

(25) Type and enter **trend**

Response: 1.tr_name:

(26) Enter a carriage return 4 times

Response: Enter Execute, Change, Substitute, Validate, or Print:

(27) Type and enter **e**

Response: FORM EXECUTED

Enter Form Name;

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.1.2.9 Back Up Incore ECD to Disk

(1) At MCC, do Steps 2 through 5.

(2) Type and enter **activate**

Response: **ACTIVATE** form displayed with cursor at

1. copy_inc_to_disk: YES

(3) Enter a carriage return

Response: **ODIN** will request the action desired.

(4) Type and enter **e**

Response: **ODIN** will return to the **DATA ENTRY** page.

(5) Type and enter **<**

Response: **RCV-199 COMPLETED**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.1.2.10 Back Up Office Dependent Data

NOTE: Before the response, there will be completed responses for each SM, the AM, and the CMP if applicable.

(1) At MCC, type and enter **BKUP:ODD;**

Response: **BKUP ODD COMPLETED**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.1.2.11 Primary Disk Backed Up

It is recommended that the primary disk be backed up and that a shelf copy of the disks be made.

(1) Back up primary disk.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.2.3.2 CALEA OUTPUT TTY GROWTH FOR 3B21D

3.5.2.3.2.1 OVERVIEW

The flexible input/output processor (FIOP) eliminates the need for adding a growth IOP when there is room for the peripheral device in an existing IOP. The FIOP is an efficient, simplified way to add or delete all of the low-level forms associated with a particular input/output processor (IOP) device.

3.5.2.3.2.2 PROCEDURE

NOTE: This procedure consists of the following subprocedures. Unless otherwise stated, the subprocedures

must be performed in the order stated.

3.5.2.3.2.2.1 Identify the Hardware Supporting the CALEA Output Interface.

The following hardware supports the CALEA Output interface:

- Teletypewriter controller (TTYC) number
- Teletypewriter (TTY) number
- IOP number
- PORT number
- Peripheral controller (PC) number.

3.5.2.3.2.2.2 Perform Port Switch

(1) At master control center (MCC), ensure terminal is in CMD mode.

(2) Type and enter **112**

Response: MCC page 112 is displayed.

(3) Is the maintenance cathode ray tube (MCRT) and/or the receive-only printer (ROP) connected to the maintenance teletypewriter peripheral controller (MTTYC) associated with the input/output processor (IOP) that is going to be removed from service?

If **YES**, continue.
If **NO**, go to **3.5.2.3.2.2.3 .**

(4) Set port switches **EQL - PCCA 0: 045-186** to the **AUTO** position if not already in the **AUTO** position.

(5) At MCC, type and enter one of the following to perform the port switch:

- **401** (switches both MCRT and ROP)
- **402** (switches ROP only)
- **403** (switches MCRT only).

(6) At MCC page 112, verify the MCRT and ROP are not connected to the selected IOP.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.2.2.3 Enter *UNIX*® Real Time Reliable (RTR) System Recent Change and Verify (RC/V)

(1) Is master control center (MCC) or RC/V terminal to be used?

MCC proceed to Step 2.

RC/V proceed to Step 8.

(2) At MCC, ensure terminal is in command mode.

(3) At MCC, do Steps 4 through 7.

(4) Type and enter CMD **199**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(5) Type and enter **incore**

Response: Cursor at **2.review only**

(6) Type and enter **n**

Response: Cursor at **3.journaling**

(7) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(8) At RC/V terminal, type and enter **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(9) Type and enter **incore**

Response: Cursor at **2.review only**

(10) Type and enter **n**

Response: Cursor at **3.journaling**

(11) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.2.2.4 Enter High-Level Forms

(1) Type and enter **toggle**

Response: Takes you to the high-level forms.

(2) Type and enter **help**

Response: List of all high-level forms available.

NOTE: While trying to grow the CALEA Output TTY, a prompt to do corrective action before continuing may appear if any of the following states are encountered:

- Attempting to grow the CALEA Output TTY in a slot with a device in the equip state.
- The slot selected has a device in the unequip state.

If any of the previously mentioned states are present, the high-level delete form must be executed. The procedures for deleting existing forms are in 235-105-331, *5ESS® Switch Hardware Change Procedures - Degrowth.*

(3) Type and enter **iopslots**

Response: **iopslots** form displayed.
Cursor at **1. unit_name:**

(4) Type and enter **IOP**

Response: Cursor at **unit_number:**

(5) Type and enter appropriate unit number (**0**, **1**, **2**, or **3**).

Response: List of all IOP slots assigned.

(6) Type and enter **<**

Response: Exit **iopslots** form.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.2.2.5 Insert TTYC Data

NOTE: An **!** may be entered any time prompted to abort the form and return to the state when the form was started.

(1) If there is an existing TTYC, a new TTYC may not have to be grown. Go to **3.5.2.3.2.2.7** .

(2) Type and enter **ttycadd**

Response: **ttycadd** form displayed.
Cursor at **1. ttyc_name:**

(3) Type and enter appropriate TTYC number.

Response: Cursor at **2. packname:**

(4) Type and enter appropriate packname (**tn74** or **un582**).

Response: Cursor at **3. slot:**

(5) Type and enter appropriate slot position.

Response: Cursor at **4. IOP_number:**

(6) Type and enter appropriate IOP number (**0**, **1**, **2** , or **3**).

Response: Cursor at **5. plu_unit_name:**

(7) Type and enter appropriate data or **CARRIAGE RETURN.**

Response: Cursor at **6. plu_unit_number:**

(8) Type and enter appropriate data or **CARRIAGE RETURN.**

(9) Type and enter **i**

(10) The low-level forms will now be added automatically.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.2.2.6 Complete TTYC Hardware Installation

NOTE: Use this procedure along with the prompts on the selected terminal.

(1) ***First prompt:*** **Remove IOP x and power it down. When complete, hit return to continue or ! to abort.**

At selected terminal, type and enter **RMV:IOP=**x**;**

Where: x = IOP number receiving the new device.

Response: **REMOVE IOP** x **COMPLETED**

At the IOP power switch, simultaneously depress the **MOR** and **OFF** switches.

Press **CARRIAGE RETURN.**

(2) ***Second prompt:*** **Install TTYC x - hit return to continue or ! to abort.**

Installation Function

Press **CARRIAGE RETURN.**

(3) ***Third prompt:*** **Power up and restore IOP x. After ATP hit return to continue or ! to abort.**

At the IOP power switch, simultaneously depress the **MOR** and **ON** switches.

At selected terminal, type and enter **RST:IOP=**x**;**

Where: x = IOP number receiving the new device.

Response: **RESTORE IOP** x **COMPLETED**

Press **CARRIAGE RETURN.**

(4) Type and enter **<**

Response: Exit the ttycadd form.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.2.2.7 Insert TTY Data

NOTE: An **!** may be entered any time prompted to abort the form and return to the state when the form was started.

(1) Type and enter **ttyadd**

Response: **ttyadd** form displayed.
Cursor at **1. tty_name:**

(2) ***Note:*** Fields not specified receive the default value by entering **CARRIAGE RETURN.**

Type and enter the following data:

1. tty_name:	enter **TTY27**
2. baud_rate:	enter (as specified or **CARRIAGE RETURN**)

3. login_term:	enter (as specified or **CARRIAGE RETURN**)
4. auth_chk:	enter (as specified or **CARRIAGE RETURN**)
5. term_type:	enter (as specified or **CARRIAGE RETURN**)
6. line_mode:	enter (as specified or **CARRIAGE RETURN**)
7. port:	enter **0**, **1**, **2**, or **3**
8. ttyc_number:	enter **TTYC** controller number
9. plu_unit_name:	enter (as specified or **CARRIAGE RETURN**)
10. plu_unit_number:	enter (as specified or **CARRIAGE RETURN**)

NOTE: If a UN582 is equipped, you are allowed to use ports 0-3.
If a TN74 is equipped, you can only use ports 2 and 3.

(3) Type and enter **i**

(4) The low-level forms will now be added automatically.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.2.2.8 Complete TTY Hardware Installation

NOTE: Use this procedure along with the prompts on the selected terminal.

(1) ***First prompt:*** **Remove IOP x from service and power down. Hit return to continue or ! to abort.**

At selected terminal, type and enter **RMV:IOP=**x**;**

Where: x = IOP number receiving the new device.

Response: **REMOVE IOP** x **COMPLETED**

At the IOP power switch, simultaneously depress the **MOR** and **OFF** switches.

Press **CARRIAGE RETURN.**

(2) ***Second prompt:*** **Physically connect TTY x. Hit return to continue or ! to abort.**

Installation Function

Press **CARRIAGE RETURN.**

(3) ***Third prompt:*** **Power up and restore IOP x. Hit return to continue or ! to abort.**

At the IOP power switch, simultaneously depress the **MOR** and **ON** switches.

At selected terminal, type and enter **RST:IOP=**x**,UCL;**

Where: x = IOP number receiving the new device.

Response: **RESTORE IOP** x **COMPLETED**

Press **CARRIAGE RETURN.**

(4) ***Fourth prompt:*** **Remove TTYC x from service. Hit return to continue or ! to abort.**

At MCC, type and enter **RMV:TTYC=**x **;**

Where: x = Appropriate controller number.

Response: **RMV TTYC** x **COMPLETED**

Press **CARRIAGE RETURN**.

(5) ***Fifth prompt:*** **Diagnose and restore TTYC x. When complete, hit return to continue or ! to abort.**

NOTE: All tests pass (ATP) must be achieved before continuing.

At MCC, type and enter **DGN:TTYC=**x**,RAW,TLP;**

Where: x = Appropriate controller number.

Response: DGN TTYC ***x*** **COMPLETED ATP**

At MCC, type and enter **RST:TTYC=**x**;**

Where: x = Appropriate controller number.

Response: **RST TTYC** x **COMPLETED**

Press **CARRIAGE RETURN**.

Response: **FORM INSERTED**

(6) Type and enter **<**

Response: Exit the ttyadd form.

(7) Type and enter **toggle**

Response: Low-level form displayed on screen.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.2.2.9 Back Up Incore ECD to Disk

(1) At MCC, do Steps 2 through 5.

(2) Type and enter **activate**

Response: **ACTIVATE** form displayed with cursor at
1. copy_inc_to_disk: YES

(3) Enter a carriage return

Response: **ODIN** will request the action desired.

(4) Type and enter **e**

Response: **ODIN** will return to the **DATA ENTRY** page.

(5) Type and enter **<**

Response: **RCV-199 COMPLETED**

3.5.2.3.2.2.10 Back Up Office Dependent Data

NOTE: Before the response, there will be completed responses for each SM, the AM, and the CMP if applicable.

(1) At MCC, type and enter **BKUP:ODD;**

Response: **BKUP ODD COMPLETED**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.2.2.11 Primary Disk Backed Up

Back up primary disk and make shelf copy of the disks.

(1) Back up primary disk.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.2.3.3 CALEA TTY DEGROWTH FOR 3B21D

3.5.2.3.3.1 PROCEDURE

NOTE: This procedure consists of the following subprocedures. Unless otherwise stated, the subprocedures must be performed in the order stated.

3.5.2.3.3.1.1 Prerequisites for Degrowth

- Ensure that both the master control center (MCC) and the receive-only printer (ROP) are ***not*** connected to the input/output processor (IOP) that is degrowing the CALEA TTY device.

3.5.2.3.3.1.2 Perform Port Switch from Selected IOP

(1) At MCC, ensure terminal is in CMD mode.

(2) Type and enter **112**

Response: MCC page 112 is displayed.

(3) Is the MCC and/or the ROP connected to the maintenance teletypewriter peripheral controller (MTTYC) associated with the IOP that is going to be removed from service?

If **YES**, then continue with Step **4.**
If **NO**, then continue with **3.5.2.3.3.1.3** .

(4) Set port switches **EQL - PCCA 0: 045-186** to the **AUTO** position if not already in the AUTO position.

(5) At MCC, type and enter one of the following to perform the port switch:

- **401** (switches both MCC and ROP)
- **402** (switches ROP only)
- **403** (switches MCC only).

(6) At MCC page 112, verify the MCC and ROP are not connected to the selected IOP.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.3.1.3 Enter *UNIX*® Real Time Reliable (RTR) System Recent Change and Verify (RC/V)

(1) Is master control center (MCC) or RC/V terminal to be used?

MCC proceed to Step 2.

RC/V proceed to Step 9.

(2) At MCC, ensure terminal is in command mode.

(3) At MCC, do Steps 4 through 8.

(4) Type and enter CMD **199**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(5) Type and enter **incore**

Response: Cursor at **2.review only**

(6) Type and enter **n**

Response: Cursor at **3.journaling**

(7) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(8) Type and enter **toggle**

Response: Will take you to the high-level forms.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE (on the MCC).

(9) At RC/V terminal, type and enter **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(10) Type and enter **incore**

Response: Cursor at **2.review only**

(11) Type and enter **n**

Response: Cursor at **3.journaling**

(12) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(13) Type and enter **toggle**

Response: Will take you to the high-level forms.

(14) Type and enter *help*

Response: List of all high-level forms available is displayed.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE (on the RC/V terminal).

3.5.2.3.3.1.4 Delete TTY Data

(1) Type and enter **ttydel**

Response: ttydel form displayed.
Cursor at **1. tty_name:**

(2) Type and enter the key value for the identified degrowth unit:

1. tty_name:**TTY26** (for CALEA Input TTY) or **TTY27** (for CALEA Output TTY)

(3) Type and enter **d**

(4) The low-level forms will now be deleted automatically, and the user will be prompted to perform certain functions.

(5) If the hardware associated with the CALEA TTY is *not* being removed, the following prompts can be omitted by entering a CARRIAGE RETURN. However, the TTYC for the CALEA TTY must be in the out-of-service (OOS) state.

NOTE: The following prompts will place the existing IOP interfaces in the OOS state. Appropriate notification should be made to the user.

(6) ***First prompt:*** Remove IOP X from service. Hit RETURN when completed.

Where: X = the IOP number that the CALEA TTY is assigned.

Action: At the OOS central processing unit (CPU) power switch (TN5 circuit pack), press the **ROS/RST** rocker switch to the **ROS** position.

Comment: IOP pack locations are given:
IOP 0 - PCCA 0 ; 033-162
IOP 1 - PCCA 1 ; 133-162

Response: The **ROS** LED lights followed by the **RQIP** LED. The **RQIP** LED is extinguished.

NOTE: If the **RQIP** LED is NOT extinguished and the **RQIP** LED flashes for 8 seconds, the request has been denied. Correct the problem before continuing.

(7) At OOS CPU, press the OFF switch.

Response: The **OFF** LED lights.

(8) Hit RETURN when complete.

(9) ***Second prompt:*** Power down and disconnect TTY X. Hit RETURN when completed.

Where: X = the TTY number of the CALEA TTY.

Action: With the power removed from the data set, disconnect the cable between the TN74B or UN582 and the data set. Disconnect the cabling between the data set and the 829A data auxiliary set and between the 829A and the Distribution Frame. Cross connects must also be disconnected from the Distribution Frame to the incoming Operational Support System (OSS) transmission line. Hit RETURN when complete.

(10) ***Third prompt:*** Return power and restore IOP X. Hit RETURN when completed.

Where: X = the IOP number that the CALEA TTY is assigned.

Action: At the selected IOP power switch, press the **ON** switch.

Comment: IOP pack locations are given:
IOP 0 - PCCA 0 ; 033-162
IOP 1 - PCCA 1 ; 133-162

Response: The **OFF** LED extinguishes.

(11) At the IOP power switch, press the **ROS/RST** switch to the **RST** position.

Response: The **ROS** LED extinguishes and the **RQIP** LED lights and extinguishes after the IOP is restored. All diagnosable units under the IOP will be diagnosed. All diagnosed units will be returned to service with the exception of the units being degrown.

Comment: All tests pass (ATP) must be achieved before continuing to subsequent procedures.

(12) Hit RETURN when complete.

(13) Is the TTYC controller to be degrown?

If **YES**, proceed to Step **14**. If **NO**, proceed to Step **16**.

(14) Type and enter **<**

Response: The ttydel form is exited.

(15) Proceed to **3.5.2.3.3.1.5** .

(16) Type and enter **<**

Response: The ttydel form is exited.

(17) Type and enter **toggle**

Response: Low-level form displayed on screen.

(18) Proceed to **3.5.2.3.3.1.6** .

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.3.1.5 Degrow the TTYC

(1) The TTY *must* be deleted before the controller that it is connected to can be deleted.

(2) Type and enter **ttycdel**

Response: The ttycdel form is displayed with cursor at **1. ttyc_name**.

(3) Type and enter the following key value for the identified degrowth unit:

1. ttyc_name: **TTYC**XX

Where: XX = appropriate TTYC indicator

(4) Type and enter **d**

Response: The low-level forms will now be deleted automatically and the user will be prompted to perform certain functions.

(5) If the TTYC associated hardware is *not* being removed, the following prompts can be omitted by entering a CARRIAGE RETURN. However, the IOP must be in the OOS state.

NOTE: The following prompts will place the existing IOP interface in the OOS state. Appropriate notification should be made to the user.

(6) ***First prompt:*** Remove and power down IOP X. Hit RETURN when completed.

Where: X = the IOP number that the CALEA TTY is assigned.

Action: At the OOS central processing unit (CPU) power switch (TN5 circuit pack), press the **ROS/RST** rocker switch to the **ROS** position.

Comment: IOP pack locations are given:
IOP 0 - PCCA 0 ; 033-162
IOP 1 - PCCA 1 ; 133-162

Response: The **ROS** LED lights followed by the **RQIP** LED. The **RQIP** LED is extinguished.

NOTE: If the **RQIP** LED is NOT and the **RQIP** LED flashes for 8 seconds, the request has been denied. Correct the problem before continuing.

(7) At OOS CPU, press the OFF switch.

Response: The **OFF** LED lights.

(8) Hit RETURN when complete.

(9) ***Second prompt:*** Physically disconnect TTYC X. Hit RETURN when completed.

Where: X = the TTYC number

Action: Remove the TTYC (TN74B or UN582) from the slot where it was assigned. Hit RETURN when complete.

(10) ***Third prompt:*** Power up IOP X and restore it. Hit RETURN when completed.

Where: X = the IOP number that the TTYC is assigned.

Action: At the selected IOP power switch, press the **ON** switch.

Response: The **OFF** LED extinguishes.

(11) At the IOP power switch, press the **ROS/RST** switch to the **RST** position.

Comment: IOP pack locations are given:
IOP 0 - PCCA 0 ; 033-162
IOP 1 - PCCA 1 ; 133-162

Response: The **ROS** LED extinguishes and the **RQIP** LED lights and extinguishes after the IOP is restored. All diagnosable units under the IOP will be diagnosed. All diagnosed units will be returned to service.

Comment: ATP must be achieved before continuing to subsequent procedures.

(12) Hit RETURN when complete.

(13) Type and enter **<**

Response: The ttycdel form is exited.

(14) Type and enter **toggle**

Response: Low-level form displayed on screen.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.3.1.6 Back Up Incore ECD to Disk

(1) At MCC, do Steps **2** through **5.**

(2) Type and enter **activate**

Response: ACTIVATE form displayed with cursor at

1. copy_inc_to_disk: YES

(3) Enter a carriage return

Response: ODIN will request the action desired.

(4) Type and enter **e**

Response: ODIN will return to the DATA ENTRY page.

(5) Type and enter **<**

Response: **RCV MENU RCVECD COMPLETED**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.3.1.7 Backup Office Dependent Data

NOTE: Before the response, there will be completed responses for each SM, the AM, and the CMP if applicable.

(1) At MCC, type and enter **BKUP:ODD;**

Response: **BKUP ODD COMPLETED**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

3.5.2.3.3.1.8 Back Up Primary Disk

It is recommended that the primary disk be backed up and a shelf copy made of the disks.

(1) Backup primary disk partitions and make a shelf copy.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.2.3.4 CALEA INPUT TTY GROWTH FOR VCDX OR DRM

PROCEDURE

NOTE: This procedure consists of the following subprocedures. Unless otherwise stated, the subprocedures must be performed in the order stated.

(1) Enter *UNIX*® RTR Recent Change and Verify.

(a) Is MCC or STLWS terminal to be used?

For MCC, proceed to Step **b.**
For STLWS proceed to Step **i**.

(b) At MCC, ensure terminal is in command mode.

(c) At MCC, do Steps **d** through **h**.

(d) Type and enter: **199**

Response: **RCV PARAMETER INFO** page displayed with cursor at **1. database_name**

(e) Type and enter: **incore**

Response: **2. review only**

(f) Type and enter: **n**

Response: **3. journaling**

(g) Type and enter: *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - Data Entry page displayed.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(h) At STLWS terminal, type and enter: **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1. database_name**

(i) Type and enter **incore**

Response: Response: **2. review only**

(j) Type and enter: **n**

Response: **3. journaling**

(k) Type and enter: *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - Data Entry page displayed.

Cursor at **Enter Form Name:**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(2) Enter high-level forms.

(a) Type and enter: **toggle**

Response: Will take you to the high-level forms.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(3) Insert TTY data.

(a) Type and enter: **ttyadd**

Response: ttyadd form displayed.

Cursor at **1. tty_name:**

NOTE: An **!** may be entered any time prompted to abort the form and return to the state when the form was started.

(b) Type and enter the following data:

1. tty_name [a] :	enter TTY26
2. baud_rate:	enter (as specified or CARRIAGE RETURN)
3. login_term:	enter n
4. auth_chk:	enter t
5. term_type:	enter (as specified or CARRIAGE RETURN)
6. line_mode:	enter (as specified or CARRIAGE RETURN)
7. port:	enter 2 or 3 for TTYC port (see Tables 3-1 and 3-2)
8. ttyc_number:	enter TTYC number base on SPC/SAI port (see Tables 3-1 and 3-2)
9. plu_unit_name:	enter CARRIAGE RETURN
10. plu_unit_number:	enter CARRIAGE RETURN

Notes:

a. tty_name must be entered in all capital letters.

Table 3-1 SPARC5 Terminal Locations

S/PI No.	AW SBUS SLOT No.	SPC PORT	TTYC PORT	TTYC No.
0	3	2	2	11
0	3	3	3	11
0	3	4	2	12
0	3	5	3	12
0	3	6	2	13
0	3	7	3	13
1	1	0	2	14
1	1	1	3	14
1	1	2	2	15
1	1	3	3	15
1	1	4	2	16
1	1	5	3	16
1	1	6	2	17
1	1	7	3	17

Table 3-2 Ultra Terminal Locations

S/PI No.	AW PCI SLOT No.	SAI PORT	TTYC PORT	TTYC No.
0	1	2	2	11
0	1	3	3	11
0	1	4	2	12
0	1	5	3	12
0	1	6	2	13
0	1	7	3	13
1	2	0	2	14
1	2	1	3	14
1	2	2	2	15
1	2	3	3	15
1	2	4	2	16
1	2	5	3	16
1	2	6	2	17
1	2	7	3	17

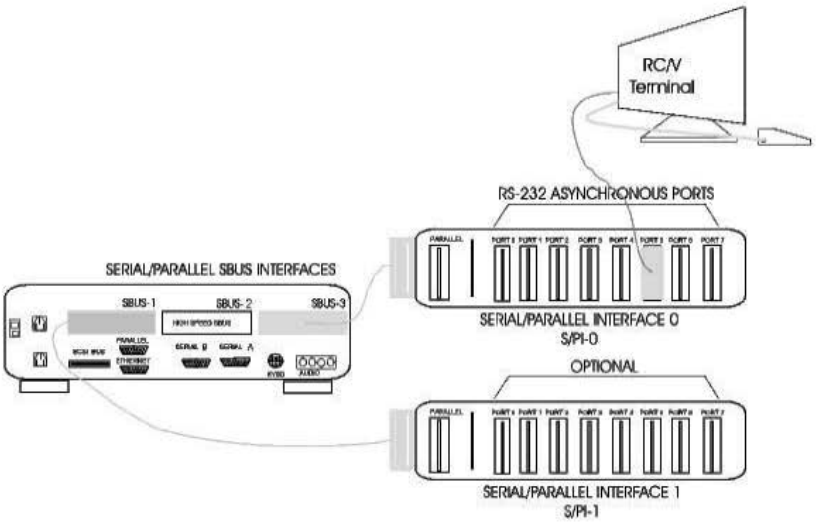
NOTE: Fields not specified receive the default value by entering CARRIAGE RETURN.

NOTE: When growing a TTY terminal, a defensive check failure message **REPT CONFIG FAULT Assert = 412** may be received. This failure message may be ignored.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(4) Install the CALEA input TTY to the SAI/SPC port corresponding to the TTYC port and TTYC number chosen in Tables 3-1 and 3-2 .

See Figures 3-2 (SPARC5 terminal) and 3-3 (Ultra terminal) for a graphical representation of the connections.



ADMINISTRATIVE WORKSTATION (Rear View)

Figure 3-2 Surveillance Administration Terminal Installation (SPARC5)

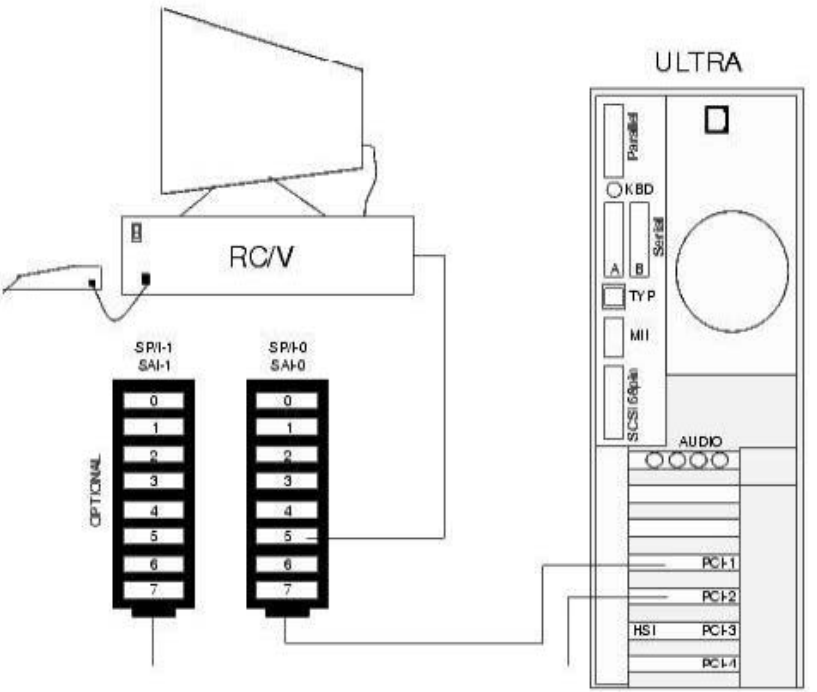


Figure 3-3 Surveillance Administration Terminal Installation (Ultra)

(a) Enter CARRIAGE RETURN.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(5) Restore TTY x to service.

(a) At MCC, type and enter the appropriate message:

RST:TTY=x

Where:

x= appropriate TTY number.

Response: **RST TTY** x **COMPLETED**

(b) Enter CARRIAGE RETURN.

Response: **FORM INSERTED**

(c) Type and enter: **<**

Response: Exit the ttyadd form.

(d) Type and enter: **trbegin**

Response: **1.tr_name**

(e) Enter carriage return

Response: **Enter Execute, Change, Substitute, Validate, or Print:**

(f) Type and enter **e**

Response: **Enter Form Name:**

(g) Type and enter: **authdef**

Response: **I=Insert R=Review U=Update D=Delete :**

(h) Type and enter: **u**

Response: **1.comgr_name:**

(i) Type and enter: **SURLEA**

Response: **Enter Update, Change, Substitute, Validate or Print:**

(j) Type and enter: **c**

Response: **Change field:**

(k) Type and enter: **5**

Response: **5.log_flag**

(l) Type and enter: **y**

Response: **Change field:**

(m) Type and enter: **8**

Response: **8.log_flag**

(n) Type and enter: **y**

Response: **Change field:**

(o) Enter a carriage return

Response: **Enter Update, Change, Substitute, Validate or Print:**

(p) Type and enter: **u**

Response: **1.comgr_name:**

(q) Type and enter: **SECLEA**

Repeat Steps (j) through (p)

(r) Type and enter: **RCV**

Repeat Steps (j) through (p)

(s) Type and enter: **FHADM**

Repeat Steps (j) through (p)

(t) Type and enter: **<**

Response: **Enter Form Name:**

(u) Type and enter: **trend**

Response: **1.tr_name:**

(v) Enter a carriage return 4 times

Response: **Enter Execute, Change, Substitute, Validate, or Print:**

(w) Type and enter: **e**

Response: **FORM EXECUTED**
Enter Form Name;

(x) Type and enter: **<**

Response: Exit this recent change session.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(6) Backup Incore ECD to disk.

(a) At MCC, do Steps **b** through **i**.

(b) Type and enter: **199**

Response: **RCV PARAMETER INFO** page displayed with cursor at **1. database_name**

(c) Type and enter: **incore**

Response: **2. review only**

(d) Type and enter: **n**

Response: **3. journaling**

(e) Type and enter: *

Response: **UNIX RTR (ODIN) - Data Entry** page displayed.

(f) Type and enter: **activate**

Response: form displayed with cursor at **1. copy_inc_to_disk: YES**

(g) Enter carriage return

Response: ODIN will request the action desired.

(h) Type and enter: **e**

Response: ODIN returns to the **UNIX RTR (ODIN) - Data Entry** page.

(i) Type and enter: **<**

Response: **RCV MENU RCV ECD COMPLETED**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(7) Backup Office Dependent Data.

NOTE: Prior to the response there will be completed responses for the switching module and the AM.

(a) At MCC, type and enter: **BKUP:ODD**

Response: **BKUP ODD COMPLETED**
It is recommended that primary disk be backed up and that a shelf copy of the disks be made.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.2.3.5 CALEA OUTPUT TTY GROWTH FOR VCDX OR DRM

PROCEDURE

NOTE: This procedure consists of the following subprocedures. Unless otherwise stated, the subprocedures must be performed in the order stated.

(1) Enter *UNIX*® RTR Recent Change and Verify.

(a) Is MCC or STLWS terminal to be used?

For MCC, proceed to Step **b.**
For STLWS proceed to Step **h.**

(b) At MCC, ensure terminal is in command mode.

(c) At MCC, do Steps **d** through **g**.

(d) Type and enter: **199**

Response: **RCV PARAMETER INFO** page displayed with cursor at **1. database_name**

(e) Type and enter: **incore**

Response: **2. review only**

(f) Type and enter: **n**

Response: **3. journaling**

(g) Type and enter: *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - Data Entry page displayed.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(h) At STLWS terminal, type and enter: **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1. database_name**

(i) Type and enter **incore**

Response: **2. review only**

(j) Type and enter: **n**

Response: **3. journaling**

(k) Type and enter: *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - Data Entry page displayed.

Cursor at **Enter Form Name:**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(2) Enter high-level forms.

(a) Type and enter: **toggle**

Response: Will take you to the high-level forms.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(3) Insert TTY data.

(a) Type and enter: **ttyadd**

Response: ttyadd form displayed.

Cursor at **1. tty_name:**

NOTE: An **!** may be entered any time prompted to abort the form and return to the state when the form was started.

(b) Type and enter the following data:

1. tty_name [a] :	enter TTY27
2. baud_rate:	enter (as specified or CARRIAGE RETURN)
3. login_term:	enter (as specified or CARRIAGE RETURN)
4. auth_chk:	enter (as specified or CARRIAGE RETURN)
5. term_type:	enter (as specified or CARRIAGE RETURN)
6. line_mode:	enter (as specified or CARRIAGE RETURN)
7. port:	enter 2 or 3 for TTYC port (see Tables 3-3 and 3-4)
8. ttyc_number:	enter TTYC number base on SPC/SAI port (see Tables 3-3 and 3-4)
9. plu_unit_name:	enter CARRIAGE RETURN
10. plu_unit_number:	enter CARRIAGE RETURN
Notes:	

a. tty_name must be entered in all capital letters.

Table 3-3 SPARC5 Terminal Locations

S/PI No.	AW SBUS SLOT No.	SPC PORT	TTYC PORT	TTYC No.
0	3	2	2	11
0	3	3	3	11
0	3	4	2	12
0	3	5	3	12
0	3	6	2	13
0	3	7	3	13
1	1	0	2	14
1	1	1	3	14
1	1	2	2	15
1	1	3	3	15
1	1	4	2	16
1	1	5	3	16
1	1	6	2	17
1	1	7	3	17

Table 3-4 Ultra Terminal Locations

S/PI No.	AW PCI SLOT No.	SAI PORT	TTYC PORT	TTYC No.
0	1	2	2	11
0	1	3	3	11
0	1	4	2	12
0	1	5	3	12
0	1	6	2	13
0	1	7	3	13
1	2	0	2	14
1	2	1	3	14
1	2	2	2	15
1	2	3	3	15
1	2	4	2	16
1	2	5	3	16
1	2	6	2	17
1	2	7	3	17

NOTE: Fields not specified receive the default value by entering CARRIAGE RETURN.

NOTE: When growing a TTY terminal a defensive check failure message REPT CONFIG FAULT Assert = 412 may be received. This failure message may be ignored.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(4) Install the traffic printer to the SAI/SPC port corresponding to the TTYC port and TTYC number chosen in Tables 3-3 and 3-4 .

See Figures 3-4 (SPARC5) and 3-5 (Ultra) for a graphical representation of the connections.

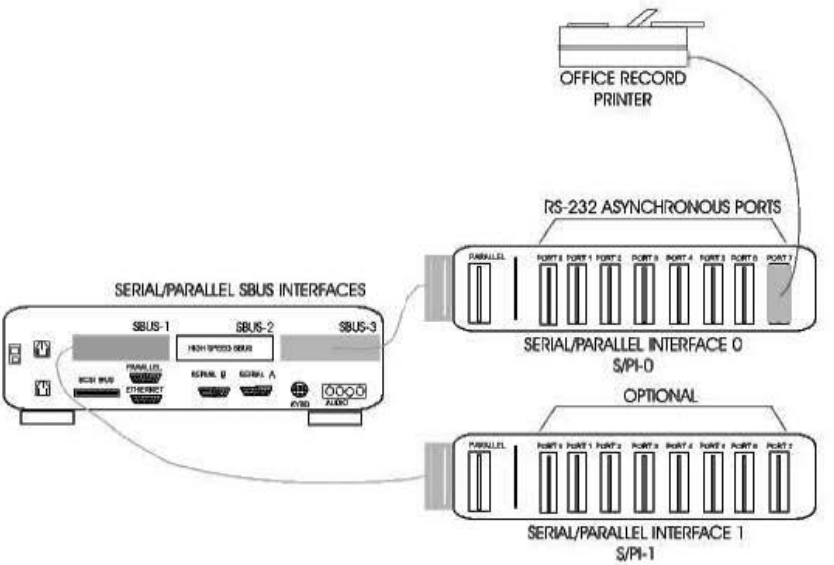


Figure 3-4 Surveillance Administration Printer Installation (SPARC5)

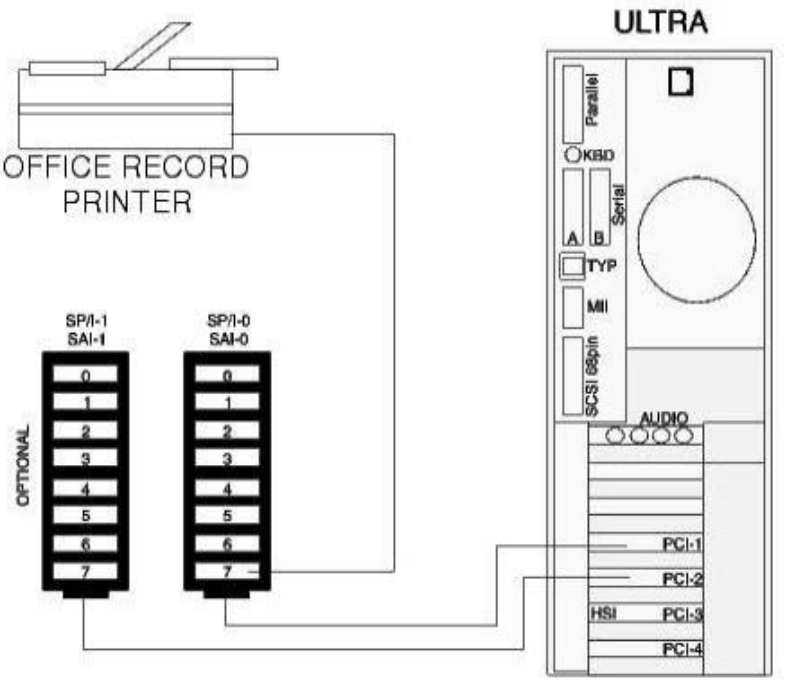


Figure 3-5 Surveillance Administration Printer Installation (ULTRA)

(a) Enter CARRIAGE RETURN.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(5) Restore TTYx to service.

(a) At MCC, type and enter the appropriate message:

RST:TTY=x

Where:

x= appropriate TTY number.

Response: RST TTY x COMPLETED

(b) Enter CARRIAGE RETURN.

Response: **FORM INSERTED**

(c) Type and enter: **<**

Response: Exit the ttyadd form.

(d) Type and enter: **<**

Response: Exit this recent change session.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(6) Backup Incore ECD to disk.

(a) At MCC, do Steps **b**through **i**.

(b) Type and enter: **199**

Response: **RCV PARAMETER INFO** page displayed with cursor at **1. database_name**

(c) Type and enter: **incore**

Response: **2. review only**

(d) Type and enter: **n**

Response: **3. journaling**

(e) Type and enter: *

Response: **UNIX RTR (ODIN) - Data Entry** page displayed.

(f) Type and enter: **activate**

Response: form displayed with cursor at **1. copy_inc_to_disk: YES**

(g) Enter carriage return

Response: ODIN will request the action desired.

(h) Type and enter: **e**

Response: ODIN returns to the **UNIX RTR (ODIN) - Data Entry** page.

(i) Type and enter: **<**

Response: **RCV MENU RCV ECD COMPLETED**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(7) Backup Office Dependent Data.

NOTE: Prior to the response there will be completed responses for the switching module and the AM.

(a) At MCC, type and enter: **BKUP:ODD**

Response: **BKUP ODD COMPLETED** It is recommended that primary disk be backed up and that a shelf copy of the disks be made.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.2.3.6 CALEA TTY DEGROWTH FOR VCDX OR DRM

PROCEDURE

NOTE: This procedure consists of the following subprocedures. Unless otherwise stated, the subprocedures must be performed in the order stated.

(1) Remove TTY x from service.

(a) At MCC, type and enter the appropriate message:

RMV:TTY=x

Where:
x = appropriate TTY number.

Response: **RMV TTY x COMPLETED**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(2) Enter *UNIX*® RTR Recent Change and Verify.

(a) Is MCC or STLWS terminal to be used?

For MCC, proceed to Step **b.**
For STLWS proceed to Step **i**.

(b) At MCC, ensure terminal is in command mode.

(c) At MCC, do Steps **d** through **h**.

(d) Type and enter: **199**

Response: **RCV PARAMETER INFO** page displayed with cursor at **1. database_name**

(e) Type and enter: **incore**

Response: **2. review only**

(f) Type and enter: **n**

Response: **3. journaling**

(g) Type and enter: *

Response: RCV INITIALIZATION IN PROGRESS message displayed. **UNIX RTR RCV (ODIN) - Data Entry** page displayed.

(h) You have completed Enter *UNIX*® RTR Recent Change and Verify, proceed to Step **3**.

(i) At STLWS terminal, type and enter: **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1. database_name**

(j) Type and enter: **incore**

Response: **2. review only**

(k) Type and enter: **n**

Response: **3. journaling**

(l) Type and enter: *

Response: RCV INITIALIZATION IN PROGRESS message displayed. **UNIX RTR RCV (ODIN) - Data Entry** page displayed. Cursor at Enter Form Name:

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(3) Enter high-level forms.

(a) Type and enter: **toggle**

Response: Will take you to the high-level forms.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(4) Delete TTY data.

(a) Type and enter: **ttydel**

Response: ttydel form displayed. Cursor at **1. tty_name:**

(b) Type and enter: **TTY26 (for CALEA Input TTY) or TTY27 (for CALEA Output TTY)**

Response: Remaining fields will automatically be completed.

(c) Type and enter: **d**

NOTE: When degrowing a TTY terminal a defensive check failure message REPT CONFIG FAULT Assert = 412 may be received. This failure message may be ignored.

(d) The low-level forms will now be deleted automatically, and the user will be prompted to perform certain functions.

(e) Type and enter: **<**

Response: Exit the ttydel form.

(f) Type and enter: **<**

Response: Exit this recent change session.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(5) Backup Incore ECD to disk.

(a) At MCC, do Steps **b** through **i**.

(b) Type and enter: **199**

Response: **RCV PARAMETER INFO** page displayed with cursor at **1. database_name**

(c) Type and enter: **incore**

Response: **2. review only**

(d) Type and enter: **n**

Response: **3. journaling**

(e) Type and enter: *

Response: **UNIX RTR (ODIN) - Data Entry** page displayed.

(f) Type and enter: **activate**

Response: ACTIVATE form displayed with cursor at **1. copy_inc_to_disk:**

(g) Type and enter: **yes**

Response: ODIN will request the action desired.

(h) Type and enter: **e**

Response: ODIN returns to the **UNIX RTR (ODIN) - Data Entry** page.

(i) Type and enter: **<**

Response: **RCV MENU RCV ECD COMPLETED**

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

(6) Backup Office Dependent Data.

NOTE: Prior to the response there will be completed responses for the switching module and the AM.

(a) At MCC, type and enter: **BKUP:ODD**

Response: **BKUP ODD COMPLETED**

It is recommended that primary disk be backed up and that a shelf copy of the disks be made.

STOP. YOU HAVE COMPLETED THIS SUBPROCEDURE.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.2.3.7 CONVERT EXISTING RC/V TTY TO CALEA INPUT TTY

3.5.2.3.7.1 STEP 1 - Identify the TTY letter of TTY to be converted.

Certain low-level ECD forms will be modified by this procedure and the TTY letter must be known. The dbinfo form will be used to determine this information, but this must be done before you begin a transaction.

NOTE: Procedure steps 1 through 22 (that is, all of "STEP 1") can be replaced by referencing the 235-080-100, *Translations Guide (TG5)*, DIV 8 (Engineering Assignments), SEC. 8 (5706 RECORD), subsection FORM AND RECORD ENTRIES, sub-subsection FLEXIBLE IOP

SELECTION, DEVICE TYPE, TTY Device Type/Device Name Cross-Reference Table, which lists device type and alias.

Procedure

(1) Is master control center (MCC) or RC/V terminal to be used?

MCC proceed to Step 2.

RC/V proceed to Step 8.

(2) At MCC, ensure terminal is in command mode.

(3) At MCC, do Steps 4 through 7.

(4) Type and enter CMD **199**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(5) Type and enter **incore**

Response: Cursor at **2.review only**

(6) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message is displayed.
UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(7) Continue with Step 11.

(8) At RC/V terminal, type and enter **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(9) Type and enter **incore**

Response: Cursor at **2.review only**

(10) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(11) Type and enter **dbinfo**

Response: DBINFO page is displayed

(12) Type and enter **/tmp/dbinf**

Response: 2. ucb_list

(13) Type and enter **<**

Response: **8.iop_list:**

(14) Type and enter **14. pointer_list**

Response: page 3 of DBINFO

14.pointer_list:

(15) Type and enter **y**

Response: **15.form_type:**

(16) Type and enter **ucb**

Response: **keyfield1:**

(17) Enter carriage return 2 times

Response: **keyfield3:**

(18) Type and enter **TTY**

Response: **keyfield4:**

(19) Type and enter **[number]** of TTY to be converted

Response: **21.get_form_rid:**

(20) Type and enter *

Response: **FORM EXECUTED**

(21) Type and enter **<**

Response: **EXIT RCV ECD**

(22) View the output file from the dbinfo form with the input message:

DUMP:FILE,ALL,FN="/tmp/dbinf"

Sample /tmp/dbinf output:

```
**************  POINTER LIST  **************

 Type of form pointed to:  ucb
 Key of form pointed to :  TTY [number of TTY to be converted]

 Records containing links to the given record.

 Form Type        Form Key

  mdct             tty[letter of TTY to be converted]
  ucb               TTYC [number of TTYC to be converted]

**************  end of sample **************
```

NOTE: Record the tty [letter of TTY to be converted] of the mdct Form Key. This will be needed later in the procedure.

3.5.2.3.7.2 STEP 2 - Modify Low-Level ECD Forms

Several low-level ECD forms will be modified by this procedure. In order for this procedure to be applicable for any RC/V TTY, some data changes may already be present.

NOTE: If the CALEA input TTY will be converted back to the original RC/V TTY, record the existing ECD data fields described in this procedure. Then follow this procedure and reinsert the original ECD data values.

Required Conditions

Before beginning procedure, remove TTY from service.

At selected terminal, type and enter **RMV:TTY**=x;

Where: x = TTY to be converted
Response: **RMV TTY x COMPLETED**

Procedure

(1) Is master control center (MCC) or RC/V terminal to be used?

MCC proceed to Step 2.

RC/V proceed to Step 9.

(2) At MCC, ensure terminal is in command mode.

(3) At MCC, do Steps 4 through 9.

(4) Type and enter CMD **199**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(5) Type and enter **incore**

Response: Cursor at **2.review only**

(6) Type and enter **n**

Response: **3.journaling**

(7) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(8) CONTINUE WITH STEP 13.

(9) At RCV terminal, type and enter: **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(10) Type and enter **incore**

Response: **2.review only**

(11) Type and enter **n**

Response: **3.journaling**

(12) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(13) Type and enter **trbegin**

Response: **1.tr_name**

(14) Enter a carriage return

Response: **Enter Execute, Change, Substitute, Validate, or Print:**

(15) Type and enter **e**

Response: **Enter Form Name:**

(16) Type and enter **getty**

Response: **I=Insert R=Review U=Update D=Delete :**

(17) **u**

Response: **1.gettyrec:**

(18) Type and enter **getty** [TTY letter from dbinfo]

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(19) Type and enter **c**

Response: **Change field:**

(20) Type and enter **gettyname**

Response: **2.gettyname:**

(21) Type and enter **shlgetty**

Response: **Change field:**

(22) Type and enter **getty_dir**

Response: **3.getty_dir:**

(23) Type and enter **/cft/shl**

Response: **Change field:**

(24) Type and enter **shlname**

Response: **4.shlname:**

(25) Type and enter **/cft/bin/pdshl.app**

Response: **Change field:**

(26) Type and enter **auth_chk**

Response: **10.auth_chk:**

(27) Type and enter **t**

Response: **Change field:**

(28) Type and enter **cmd_log**

Response: **11.cmd_log:**

(29) Type and enter **y**

Response: **Change field:**

(30) Enter a carriage return

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(31) Type and enter **u**

Response: **1.gettyrec:**

(32) Type and enter **<**

Response: **Enter Form Name:**

(33) Type and enter **ciopt**

Response: **I=Insert R=Review U=Update D=Delete :**

(34) Type and enter **u**

Response: **1.option_name:**

(35) Type and enter **ttyop**[TTY number]

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(36) Type and enter **c**

Response: **Change field:**

(37) Type and enter **cdopt_name**

Response: **3.cdopt_name:**

(38) Type and enter **VT100DAP**

Response: **Change field:**

(39) Enter a carriage return

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(40) Type and enter **u**

Response: **1.option_name:**

(41) Type and enter **<**

Response: **Enter Form Name:**

(42) Type and enter **authdef**

Response: **I=Insert R=Review U=Update D=Delete :**

(43) Type and enter **u**

Response: **1.comgr_name:**

(44) Type and enter **SURLEA**

Response: **Enter Update, Change, Substitute, Validate or Print:**

(45) Type and enter **c**

Response: **Change field:**

(46) Type and enter **5**

Response: **5.log_flag**

(47) Type and enter **y**

Response: **Change field:**

(48) Type and enter **8**

Response: **8.log_flag**

(49) Type and enter **y**

Response: **Change field:**

(50) Enter a carriage return

Response: **Enter Update, Change, Substitute, Validate or Print:**

(51) Type and enter **u**

Response: **1.comgr_name:**

(52) Type and enter **SECLEA**

Response: Repeat Steps 43 through 49

(53) Type and enter **RCV**

Response: Repeat Steps 43 through 49

(54) Type and enter **FHADM**

Response: Repeat Steps 43 through 49

(55) Type and enter **<**

Response: **Enter Form Name:**

(56) Type and enter **trend**

Response: **1.tr_name:**

(57) Enter a carriage return 4 times

Response: **Enter Execute, Change, Substitute, Validate, or Print:**

(58) Type and enter **e**

Response: **FORM EXECUTED**

Enter Form Name:

(59) Restore TTY to service.

At selected terminal, type and enter **RST:TTY=**x;

Where: x = TTY to be converted

Response: **RST TTY x COMPLETED**

3.5.2.3.7.3 STEP 3 - Back Up Incore ECD to Disk

Procedure

(1) Type and enter **activate**

Response: ACTIVATE form displayed with cursor at **1. copy_inc_to_disk: YES**

(2) Enter a carriage return

Response: ODIN will request the action desired.

(3) Type and enter **e**

Response: ODIN will return to the DATA ENTRY page.

(4) Type and enter **<**

Response: **EXIT RCV ECD**

3.5.2.3.7.4 STEP 4 - Back Up Office Dependent Data

NOTE: Before the response, there will be completed responses for each SM, the AM, and the CMP if applicable.

Procedure

(1) At MCC, type and enter **BKUP:ODD;**

Response: **BKUP ODD COMPLETED**

3.5.2.3.7.5 STEP 5 - Back Up Primary Disk and Make Shelf Copy

It is recommended that the primary disk be backed up and that a shelf copy of the disks be made.

1. Backup primary disk.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.2.3.8 CONVERT EXISTING RC/V TTY TO CALEA OUTPUT TTY

3.5.2.3.8.1 STEP 1 - Identify the TTY letter of TTY to be converted.

Certain low-level ECD forms will be modified by this procedure and the TTY letter must be known. The dbinfo form will be used to determine this information, but this must be done before you begin a transaction.

NOTE: Procedure steps 1 through 22 (that is, all of "STEP 1") can be replaced by referencing the

235-080-100, *Translations Guide (TG5)*, DIV 8 (Engineering Assingments), SEC. 8 (5706 RECORD), subsection FORM AND RECORD ENTRIES, sub-subsection FLEXIBLE IOP SELECTION, DEVICE TYPE, TTY Device Type/Device Name Cross-Reference Table, which lists device type and alias.

Procedure

(1) Is master control center (MCC) or RCV terminal to be used?

MCC proceed to Step 2.

RCV proceed to Step 8.

(2) At MCC, ensure terminal is in command mode.

(3) At MCC, do Steps 4 through 7.

(4) Type and enter CMD **199**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(5) Type and enter **incore**

Response: Cursor at **2.review only**

(6) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message is displayed.
UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(7) Continue with Step 11.

(8) At RCV terminal, type and enter **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(9) Type and enter **incore**

Response: Cursor at **2.review only**

(10) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(11) Type and enter **dbinfo**

Response: DBINFO page is displayed

(12) Type and enter **/tmp/dbinf**

Response: page 2 of DBINFO

(13) Type and enter **<**

Response: **8.iop_list:**

(14) Type and enter **<**

Response: page 3 of DBINFO

14.pointer_list:

(15) Type and enter **y**

Response: **15.form_type:**

(16) Type and enter **ucb**

Response: **keyfield1:**

(17) Enter a carriage return 2 times

Response: **keyfield3:**

(18) Type and enter **TTY**

Response: **keyfield4:**

(19) Type and enter **[number]** of TTY to be converted

Response: **21.get_form_rid:**

(20) Type and enter *

Response: **FORM EXECUTED**

(21) Type and enter **<**

Response: **EXIT RCV ECD**

(22) View the output file from the dbinfo form with the input message:

DUMP:FILE,ALL,FN="/tmp/dbinf"

```
Sample /tmp/dbinf output:

***************  POINTER LIST  ***************


 Type of form pointed to:  ucb
 Key of form pointed to :  TTY [number of TTY to be converted]

 Records containing links to the given record.

 Form Type       Form Key

  mdct            tty[letter of TTY to be converted]
  ucb              TTYC [number of TTY to be converted]

***************  end of sample ***************
```

NOTE: Record the tty [letter of TTY to be converted] of the mdct Form Key. This will be needed later in the procedure.

3.5.2.3.8.2 STEP 2 - Modify Low-Level ECD Forms

Several low-level ECD forms will be modified by this procedure. In order for this procedure to be applicable for any RC/V TTY, some data changes may already be present.

NOTE: If the CALEA output TTY will be converted back to the original RC/V TTY, record the existing ECD data fields described in this procedure. Then follow this procedure and reinsert the original ECD data values.

Required Conditions

Before beginning procedure, remove TTY from service.

At selected terminal, type and enter **RMV:TTY**=x;

Where: x = TTY to be converted
Response: **RMV TTY x COMPLETED**

Procedure

(1) Is master control center (MCC) or RC/V terminal to be used?

MCC proceed to Step 2.

RC/V proceed to Step 9.

(2) At MCC, ensure terminal is in command mode.

(3) At MCC, do Steps 4 through 9.

(4) Type and enter CMD **199**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(5) Type and enter **incore**

Response: Cursor at **2.review only**

(6) Type and enter **n**

Response: **3.journaling**

(7) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(8) CONTINUE WITH STEP 13.

(9) At RCV terminal, type and enter: **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(10) Type and enter **incore**

Response: **2.review only**

(11) Type and enter **n**

Response: **3.journaling**

(12) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(13) Type and enter **trbegin**

Response: **1.tr_name**

(14) Enter a carriage return

Response: **Enter Execute, Change, Substitute, Validate, or Print:**

(15) Type and enter **e**

Response: **Enter Form Name:**

(16) Type and enter **getty**

Response: **I=Insert R=Review U=Update D=Delete :**

(17) **u**

Response: **1.gettyrec:**

(18) Type and enter **getty** [TTY letter from dbinfo]

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(19) Type and enter **c**

Response: **Change field:**

(20) Type and enter **gettyname**

Response: **2.gettyname:**

(21) Type and enter **shlgetty**

Response: **Change field:**

(22) Type and enter **getty_dir**

Response: **3.getty_dir:**

(23) Type and enter **/cft/shl**

Response: **Change field:**

(24) Type and enter **shlname**

Response: **4.shlname:**

(25) Type and enter **/cft/bin/pdshl.app**

Response: **Change field:**

(26) Type and enter **spl**

Response: **5.spl**

(27) Type and enter **y**

Response: **Change field:**

(28) Enter a carriage return

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(29) Type and enter **u**

Response: **1.gettyrec:**

(30) Type and enter **<**

Response: **Enter Form Name:**

(31) Type and enter **ciopt**

Response: **I=Insert R=Review U=Update D=Delete :**

(32) Type and enter **u**

Response: **1.option_name:**

(33) Type and enter **ttyop**[TTY number]

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(34) Type and enter **c**

Response: **Change field:**

(35) Type and enter **ttopt_name**

Response: **2.ttopt_name:**

(36) Type and enter **caleaprt**

Response: **Change field:**

(37) Type and enter **cdopt_name**

Response: **3.cdopt_name:**

(38) Type and enter **MOD40**

Response: **Change field:**

(39) Type and enter **logon_dev**

Response: **5.logon_dev**

(40) Type and enter **n**

Response: **Change field:**

(41) Enter a carriage return

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(42) Type and enter **u**

Response: **1.option_name:**

(43) Type and enter **<**

Response: **Enter Form Name:**

(44) Type and enter **classdef**

Response: **I=Insert R=Review U=Update D=Delete :**

(45) Type and enter **u**

Response: **1.class_name**

(46) Type and enter **197**

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(47) Type and enter **c**

Response: **Change field:**

(48) Type and enter **device_list**

Response: **Row:**

(49) Type and enter **1** [if 1) has value of null]

OR

20 [if 1) has value other than null]

Response: **1)** or **20)**

(50) Type and enter **tty**[TTY letter from dbinfo]

Response: **Row:**

(51) Enter a carriage return

Response: **Change field:**

(52) Enter a carriage return

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(53) Type and enter **u**

Response: **1.class_name**

(54) Type and enter **198**

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(55) Type and enter **c**

Response: **Change field:**

(56) Type and enter **device_list**

Response: **Row:**

(57) Type and enter **1** [if 1) has value of null]

OR

20 [if 1) has value other than null]

Response: **1)** or **20)**

(58) Type and enter **tty**[TTY letter from dbinfo]

Response: **Row:**

(59) Enter a carriage return

Response: **Change field:**

(60) Enter a carriage return

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(61) Type and enter **u**

Response: **1.class_name**

(62) Type and enter **<**

Response: **Enter Form Name:**

(63) Type and enter **trend**

Response: **1.tr_name:**

(64) Enter a carriage return 4 times

Response: **Enter Execute, Change, Substitute, Validate, or Print:**

(65) Type and enter **e**

Response: **FORM EXECUTED**

Enter Form Name:

(66) Restore TTY to service.

At selected terminal, type and enter **RST:TTY=**x;

Where: x = TTY to be converted

Response: **RST TTY x COMPLETED**

3.5.2.3.8.3 STEP 3 - Back Up Incore ECD to Disk

Procedure

(1) Type and enter **activate**

Response: ACTIVATE form displayed with cursor at **1. copy_inc_to_disk: YES**

(2) Enter a carriage return

Response: ODIN will request the action desired.

(3) Type and enter **e**

Response: ODIN will return to the DATA ENTRY page.

(4) Type and enter **<**

Response: **EXIT RCV ECD**

3.5.2.3.8.4 STEP 4 - Back Up Office Dependent Data

NOTE: Before the response, there will be completed responses for each SM, the AM, and the CMP if applicable.

Procedure

(1) At MCC, type and enter **BKUP:ODD;**

Response: **BKUP ODD COMPLETED**

3.5.2.3.8.5 STEP 5 - Back Up Primary Disk and Make Shelf Copy

It is recommended that the primary disk be backed up and that a shelf copy of the disks be made.

1. Backup primary disk.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.2.3.9 CONVERT EXISTING STLWS TTY TO CALEA INPUT TTY

3.5.2.3.9.1 STEP 1 - Identify the TTY letter of TTY to be converted.

Certain low-level ECD forms will be modified by this procedure and the TTY letter must be known. The dbinfo form will be used to determine this information, but this must be done before you begin a transaction.

NOTE: Procedure steps 1 through 22 (that is, all of "STEP 1") can be replaced by referencing the 235-080-100, *Translations Guide (TG5)*, DIV 8 (Engineering Assingments), SEC. 8 (5706 RECORD), subsection FORM AND RECORD ENTRIES, sub-subsection FLEXIBLE IOP SELECTION, DEVICE TYPE, TTY Device Type/Device Name Cross-Reference Table, which lists device type and alias.

NOTE: The letter for the Alias tty is case sensitive. For the STLWS there normally are 6 lower case and 8 uppercase letters that identify the Alias.

```
Name          Device Type       Alias
STLWS1           TTY11          ttyl
STLWS2           TTY12          ttym
```

```
STLWS3          TTY13          ttyn
STLWS4          TTY14          ttyo
STLWS5          TTY9           ttyj
STLWS6          TTY10          ttyk
STLWS7          TTY28          ttyC
STLWS8          TTY29          ttyD
STLWS9          TTY30          ttyE
STLWS10         TTY31          ttyF
STLWS11         TTY32          ttyG
STLWS12         TTY33          ttyH
STLWS13         TTY34          ttyI
STLWS14         TTY50          ttyY
```

NOTE: Record the tty [letter of TTY to be converted] from the Alias in the table. This will be needed later in the procedure.

Required Conditions

Before beginning procedure, remove TTY from service.

At selected terminal, type and enter RMV:TTY=x;
`Where: x = TTY to be converted`
`Response: RMV TTY x COMPLETED`

Procedure

(1) Is master control center (MCC) or RC/V terminal to be used?

MCC proceed to Step 2.

RC/V proceed to Step 8.

(2) At MCC, ensure terminal is in command mode.

(3) At MCC, do Steps 4 through 7.

(4) Type and enter CMD **199**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(5) Type and enter **incore**

Response: Cursor at **2.review only**

(6) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message is displayed.
UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(7) Continue with Step 11.

(8) At RC/V terminal, type and enter **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(9) Type and enter **incore**

Response: Cursor at **2.review only**

(10) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(11) Type and enter **dbinfo**

Response: DBINFO page is displayed

(12) Type and enter **/tmp/dbinf**

Response: 2. ucb_list

(13) Type and enter **>**

Response: **8.iop_list:**

(14) Type and enter **>**

Response: 14. pointer_list

(15) Type and enter **y**

Response: **15.form_type:**

(16) Type and enter **ucb**

Response: **keyfield1:**

(17) Enter a carriage return 2 times

Response: **keyfield3:**

(18) Type and enter **TTY**

Response: **keyfield4:**

(19) Type and enter **[number]** of TTY to be converted

Response: **21.get_form_rid:**

(20) Type and enter *

Response: **FORM EXECUTED**

(21) Type and enter **<**

Response: **EXIT RCV ECD**

(22) View the output file from the dbinfo form with the input message:

DUMP:FILE,ALL,FN="/tmp/dbinf"

```
Sample /tmp/dbinf output:

***************  POINTER LIST  ***************

 Type of form pointed to:  ucb
 Key of form pointed to :  TTY [number of TTY to be converted]

 Records containing links to the given record.

 Form Type       Form Key

  mdct            tty[letter of TTY to be converted]
  ucb              TTYC [number of TTYC to be converted]

***************  end of sample ***************
```

NOTE: Record the tty [letter of TTY to be converted] of the mdct Form Key. This will be needed later in the procedure.

3.5.2.3.9.2 STEP 2 - Modify Low-Level ECD Forms

Several low-level ECD forms will be modified by this procedure. In order for this procedure to be applicable for any TLWS TTY, some data changes may already be present.

NOTE: If the CALEA input TTY will be converted back to the original TLWS TTY, record the existing ECD data fields described in this procedure. Then follow this procedure and reinsert the original ECD data values.

Procedure to identify and remove the CD (poker) portion of the ECD forms.

(1) Is master control center (MCC) or RC/V terminal to be used?

MCC proceed to Step 2.

RCV proceed to Step 9.

(2) At MCC, ensure terminal is in command mode.

(3) At MCC, do Steps 4 through 9.

(4) Type and enter CMD **199**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(5) Type and enter **incore**

Response: Cursor at **2.review only**

(6) Type and enter **n**

Response: **3.journaling**

(7) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(8) CONTINUE WITH STEP 13.

(9) At RCV terminal, type and enter: **RCV:MENU:DATA,RCVECD;**

Response: **RCV ECD PARAMETER INFO** page displayed with cursor at **1.database name**

(10) Type and enter **incore**

Response: **2.review only**

(11) Type and enter **n**

Response: **3.journaling**

(12) Type and enter *

Response: **RCV INITIALIZATION IN PROGRESS** message displayed.

UNIX RTR RCV (ODIN) - DATA ENTRY page is displayed.

(13) Type and enter **trbegin**

Response: **1.tr_name**

(14) Enter a carriage return

Response: **Enter Execute, Change, Substitute, Validate, or Print:**

(15) Type and enter **e**

Response: **Enter Form Name:**

Procedure to identify and record the Dap getty for the TLWS.

(1) Type and enter **logdev**

Response: **I=Insert R=Review U=Update D=Delete :**

(2) Type and enter **r**

Response: **1.logical_name:**

(3) Type and enter **/dev/cd*** Where * is the letter of the tty or Alias is recorded.

Response: **Enter Review, Change-insert, Validate, or Print:**

NOTE: **Record 7.gettyid:getty*** Where * is the getty name of the TLWS Dap.

(4) Type and enter **<**

Response: **Enter Form Name:**

Procedure to delete logdev for TLWS Dap.

(1) Type and enter **logdev**

Response: **I=Insert R=Review U=Update D=Delete :**

(2) Type and enter **d**

Response: **1.logical_name:**

(3) Type and enter **/dev/cd*** Where * is the letter of the tty or Alias recorded. Same as was used in step 18.

Response: **Enter Delete, Validate, or Print:**

(4) Type and enter **d**

Response: **1.logical_name:**

(5) Type and enter **<**

Response: **Enter Form Name:**

Procedure to delete device for TLWS Dap.

(1) Type and enter **device**

Response: **I=Insert R=Review U=Update D=Delete :**

(2) Type and enter **d**

Response: **1.logical_name:**

(3) Type and enter **cd*** Where * is the letter of the tty or Alias recorded. Same as was used in step 18.

Response: **Enter Delete, Validate, or Print:**

(4) Type and enter **d**

Response: **1.logical_name:**

(5) Type and enter **<**

Response: **Enter Form Name:**

Procedure to delete getty for TLWS Dap.

(1) Type and enter **getty**

Response: **I=Insert R=Review U=Update D=Delete :**

(2) Type and enter **d**

Response: **1.gettyrec:**

(3) Type and enter **getty*** Where * is the getty name of the TLWS Dap. This should have been recorded in step 18 7.gettyid:getty*.

Response: **Enter Delete, Validate, or Print:**

(4) Type and enter **d**

Response: **1.logical_name:**

(5) Type and enter **<**

Response: **Enter Form Name:**

Procedure to update device for tty or Alias.

(1) Type and enter **device**

Response: **I=Insert R=Review U=Update D=Delete :**

(2) Type and enter **u**

Response: **1.logical_name:**

(3) Type and enter **tty*** Where * is the letter of the tty or Alias recorded.

Response: **Enter Review, Change-insert, Validate, screen#, or Print:**

(4) Type and enter **2**

Response: **Enter Review, Change-insert, Validate, screen#, or Print:**

(5) Type and enter **c**

Response: **Change field:**

(6) Type and enter **30**

Response: **30.msg_trailer**

tr1

x0

(7) Type and enter **x19**

Response: **30.msg_trailer**

tr2

x0

(8) Type and enter **15 returns**

Response: **Change field:**

(9) Type and enter **return**

Response: **I=Insert R=Review U=Update D=Delete :**

(10) Type and enter **u**

Response: **1.logical_devname:**

(11) Type and enter **<**

Response: **Enter Form Name:**

Procedure to update getty for tty or Alias

(1) Type and enter **getty**

Response: **I=Insert R=Review U=Update D=Delete :**

(2) Type and enter **u**

Response: **1.gettyrec:**

(3) Type and enter **getty (letter of the tty or Alias recorded)**

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(4) Type and enter **c**

Response: **Change field:**

(5) Type and enter **2**

Response: **2.gettyname:**

(6) Type and enter **shlgetty**

Response: **Change field:**

(7) Type and enter **3**

Response: **3.getty_dir:**

(8) Type and enter **/cft/shl**

Response: **Change field:**

(9) Type and enter **4**

Response: **4.shlname:**

(10) Type and enter **/cft/bin/pdshl.app**

Response: **Change field:**

(11) Type and enter **10**

Response: **10.auth_chk:**

(12) Type and enter **t**

Response: **Change field:**

(13) Type and enter **11**

Response: **11.cmd_log:**

(14) Type and enter **y**

Response: **Change field:**

(15) Enter a carriage return

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(16) Type and enter **u**

Response: **1.gettyrec:**

(17) Type and enter **<**

Response: **Enter Form Name:**

Procedure to update ciopt for tty

(1) Type and enter **ciopt**

Response: **I=Insert R=Review U=Update D=Delete :**

(2) Type and enter **u**

Response: **1.option_name:**

(3) Type and enter **ttyop*** Where * is the number of the tty being changed.

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(4) Type and enter **c**

Response: **Change field:**

(5) Type and enter **2**

Response: **2.ttopt_name:**

(6) Type and enter **PDS48**

Response: **Change field:**

(7) Type and enter **3**

Response: **3.cdopt_name:**

(8) Type and enter **VT100DAP**

Response: **Change field:**

(9) Enter a carriage return

Response: **Enter Update, Change, Substitute, Validate, or Print:**

(10) Type and enter **u**

Response: **1.option_name:**

(11) Type and enter **<**

Response: **Enter Form Name:**

Procedure to update authdef forms.

(1) Type and enter **authdef**

Response: **I=Insert R=Review U=Update D=Delete :**

(2) Type and enter **u**

Response: **1.comgr_name:**

(3) Type and enter **SURLEA**

Response: **Enter Update, Change, Substitute, Validate or Print:**

(4) Type and enter **c**

Response: **Change field:**

(5) Type and enter **5**

Response: **5.log_flag**

(6) Type and enter **y**

Response: **Change field:**

(7) Type and enter **8**

Response: **8.log_flag**

(8) Type and enter **y**

Response: **Change field:**

(9) Enter a **carriage return**

Response: **Enter Update, Change, Substitute, Validate or Print:**

(10) Type and enter **u**

Response: **1.comgr_name:**

(11) Type and enter **SECLEA**

Response: **Repeat Steps 77 through 83**

(12) Type and enter **RCV**

Response: **Repeat Steps 77 through 83**

(13) Type and enter **FHADM**

Response: **Repeat Steps 77 through 83**

(14) Type and enter **<**

Response: **Enter Form Name:**

(15) Type and enter **trend**

Response: **1.tr_name:**

(16) Enter a carriage return 4 times.

Response: **Enter Execute, Change, Substitute, Validate, or Print:**

(17) Type and enter **e**

Response: **FORM EXECUTED**

Enter Form Name:

(18) Type and enter **<**

(19) Restore TTY to service.

At selected terminal, type and enter RST:TTY=x;

Where: x = TTY to be converted

Response: **RST TTY x COMPLETED**

3.5.2.3.9.3 STEP 3 - Procedure to Back Up Incore ECD to Disk

(1) Type and enter **activate**

Response: ACTIVATE form displayed with cursor at **1. copy_inc_to_disk: YES**

(2) Enter a carriage return.

Response: ODIN will request the action desired.

(3) Type and enter **e**

Response: ODIN will return to the DATA ENTRY page.

(4) Type and enter **<**

Response: **EXIT RCV ECD**

3.5.2.3.9.4 STEP 4 - Procedure to Back Up Office Dependent Data

NOTE: Before the response, there will be completed responses for each SM, the AM, and the CMP if applicable.

(1) At MCC, type and enter **BKUP:ODD;**

Response: **BKUP ODD COMPLETED**

3.5.2.3.9.5 STEP 5 - Procedure to Back Up Primary Disk and Make Shelf Copy

It is recommended that the primary disk be backed up and that a shelf copy of the disks be made.

1. Backup primary disk.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.2.3.10 RELATED INFORMATION

See 235-105-231, *5ESS® Switch Hardware Maintenance Procedures - Growth* and 235-600-314, *5ESS® Switch ECD/SG Data Base Manual*, for other growth-related information.

See 235-120-010, *CDX Reference Guide*, 235-120-120, *VCDX User's Guide*, and 235-105-510, *3B21D Computer Hardware Reference Manual* for more information regarding TTY interface specifications.

3.5.3 AUTHORITY CLASS ASSIGNMENT

3.5.3.1 OVERVIEW

Security and surveillance terminal authority classes must be assigned to the CALEA TTYs. The following commands assume the provisioning of the SAS terminal and ROP as follows:

Device Type	Name	Alias
TTY26	CALEASAS	tty9
TTY27	CALEAPRT	ttyx

NOTE: If TTYs other than TTY26 and TTY27 have been provisioned for CALEA (such as existing TTYs temporarily converted for CALEA use), then those TTY numbers must be entered.

NOTE: The ADD and VFY commands must be executed from a terminal with an authority class of AUTH assigned.

3.5.3.2 PROCEDURE

NOTE: The TERM numbers entered via the commands in this procedure must be the same as the TERM

numbers assigned for the CALEA TTYs. If TTYs other than TTY26 and TTY27 have been provisioned for CALEA, those TTY numbers must be entered.

(1) Remove the CALEA TTYs.

Type and enter the commands:
RMV:TTY=26;
RMV:TTY=27;

Response: **RMV TTY a b**

Where:
a = Terminal ID (device type)
b = Termination status.

(2) Add terminal authority class and terminal command groups for both CALEA TTYs.

Type and enter these commands:

ADD:TAUTH:TERM="tty9";

ADD:TAUTH:TERM="ttyx";

ADD:TCGRP:TERM="tty9",COMGR=FHADM;

ADD:TCGRP:TERM="ttyx",COMGR=FHADM;

ADD:TCGRP:TERM="tty9",COMGR=SECLEA;

ADD:TCGRP:TERM="ttyx",COMGR=SECLEA;

ADD:TCGRP:TERM="tty9",COMGR=SURLEA;

ADD:TCGRP:TERM="ttyx",COMGR=SURLEA;

ADD:TCGRP:TERM="tty9",COMGR=RCV;

ADD:TCGRP:TERM="ttyx",COMGR=RCV;

Response: Standard system responses.

(3) Verify that the new authority classes were added.

Type and enter **VFY:TAUTH;**

Response: **VFY TAUTH**

TERM

a

Where

a = Terminal ID.

(4) Verify that the new terminal-command groups were added.

Type and enter the commands:
VFY:TCGRP:TERM="ttyx";
VFY:TCGRP:TERM="tty9";

Response: **VFY TCGRP**

TERM PROFILE COMGR

a b c

Where:
a = Terminal ID (alias)
b = Profile identity
c = Command group.

(5) Restart the TTYs.

Type and enter the commands:
RST:TTY=26;
RST:TTY=27;

Response: **RST TTY a b**

Where:
a = Terminal ID (device type)
b = Termination status.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.4 ASSIGN SAS TERMINAL ACCESS TO NON-CALEA VIEWS (5E15 and later)

3.5.4.1 OVERVIEW

Beginning with the 5E15 software release, the CALEA Punchlist feature allows for the Surveillance Administrator using the SAS terminal to have full access (read, update, delete, insert [RUDI] permissions) to non-CALEA views (classes A through 33). Access is permitted by switch maintenance personnel setting the **ADMIN ACCESS** field on Recent Change view 8.1 to **Y** (the default value is "N").

```
5ESS SWITCH
SCREEN 13 OF 15                          RECENT CHANGE  8.1
(5509)                          OFFICE PARAMETERS (MISCELLANEOUS)

227. ACCT PROMPT      _______     235. CALEA SM      _
228. CARRIER TONE     _           236. ADMIN ACCESS  Y
229. NSC WC ID        ___         237. TD LIMIT      __
```

```
230. ORIG NSC        ___
231. TERM NSC        ___
232. TEST CALL TNSC  ___

    INCREASED TGN
233. MAX TGN    ____
234. MAX RTIDX  _____
```

3.5.4.2 PROCEDURE

(1) Activate a Recent Change session at a non-CALEA terminal.

Type and enter **RCV:MENU:APPRC;**

Response: A Recent Change session is started and the Main Menu appears.

(2) Access view 8.1 by entering **8.1u**

Response: View 8.1 appears with the cursor in the OFFICE ID key field.

(3) Enter the office identifier followed by a carriage return.

Response: View 8.1 appears with all currently-defined fields filled in.

(4) Enter **C** (for the "change" operation) followed by a carriage return. The cursor is positioned at the 'Change Field" prompt at the bottom of the screen. Enter **ADMIN ACCESS** to position the cursor at the ADMIN ACCESS field. Enter **Y** followed by a carriage return. The screen will look something like this:

```
5ESS SWITCH
SCREEN 13 OF 15                          RECENT CHANGE  8.1
(5509)                          OFFICE PARAMETERS (MISCELLANEOUS)

227. ACCT PROMPT     _______     235. CALEA SM  4
228. CARRIER TONE    _           236. ADMIN ACCESS Y
229. NSC WC ID       ___         237. TD LIMIT     50
230. ORIG NSC        ___
231. TERM NSC        ___
232. TEST CALL TNSC  ___

    INCREASED TGN
233. MAX TGN    ____
234. MAX RTIDX  _____
```

Response: Field ADMIN ACCESS changed to "Y".

(5) Type * or **U** to update the view in the database.

Response: **updating...**

followed by **FORM UPDATED**

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.5.5 SECURITY ADMINISTRATOR LOGIN AND PASSWORD ADMINISTRATION

3.5.5.1 PURPOSE

The switch administrator is responsible for assigning and deleting Security Administrator logins and updating the Security Administrator passwords.

Security Administrator login and password assignment should be done as soon as possible after activating the CALEA feature so that the Security Administrator will have time to complete the required security administration procedures prior to a court order being received by the service provider.

3.5.5.2 SECURITY ADMINISTRATOR LOGIN ASSIGNMENT PROCEDURE

From a non-CALEA terminal, a *5ESS*® switch Administrator must assign a login ID/password for the CALEA Security Administrator.

(1) Type and enter: **ASGN:SECRTY,USRID="a";**

Where:
a = The user ID from 3 to 8 characters in length.

Response: **Enter Password (6 to 12 characters):**

Type the password and press the "Enter" key. The following report will appear:

ASGN SECRTY
a

Where:
a = Status of the command.

(2) Verify the login by executing the command:

VFY:SECRTY;

Response:
VFY SECRTY
a

USER ID TYPE
b SECURITY ADMINISTRATOR

Where:
a = Status of the command.
b = User ID of Security Administrator(s).

3.5.5.3 SECURITY ADMINISTRATOR LOGIN DELETION PROCEDURE

From a non-CALEA terminal, a *5ESS*® switch Administrator must delete a login ID for the CALEA Security Administrator.

(1) Type and enter: **DEL:SECRTY,USRID="a";**

Where:
a = The user ID from 3 to 8 characters in length.

Response:
DEL SECRTY
a

Where:
a = Status of the command.

(2) Verify the login deletion by executing the command:

VFY:SECRTY;

Response:
VFY SECRTY
a

USER ID TYPE
b SECURITY ADMINISTRATOR

Where:
a = Status of the command.
b = User ID of Security Administrator(s).

3.5.5.4 SECURITY ADMINISTRATOR PASSWORD UPDATE PROCEDURE

If a Security Administrator forgets the password, or the password has become compromised, the password must be updated by a *5ESS*® switch Administrator. This procedure is executed from a non-CALEA terminal.

(1) Type and enter: **UPD:SECRTY,USRID="a";**

Where:
a = The user ID from 3 to 8 characters in length.

Response: **Enter Password (6 to 12 characters):**

Type the new password and press the "Enter" key. The following report will appear:

UPD SECRTY
a

Where:
a = Status of the command.

NOTE: See Chapter 6 for a complete description of these commands and reports.

3.6 TONE DECODER GROWTH (5E15 and later)

3.6.1 OVERVIEW

The CALEA Punchlist feature increases the usage of tone decoders. This increased usage may result in the need to grow additional tone decoders in the office.

3.6.2 PROCEDURE

Refer to 235-105-231, *5ESS® Switch Hardware Maintenance Procedures - Growth* for tone decoder growth procedures.

3.7 PROVISIONING THE TONE DECODER THRESHOLD (5E15 and later)

3.7.1 OVERVIEW

Beginning with the 5E15 software release, Recent Change view 8.1 has a new field (**TD LIMIT**) which allows switch personnel to specify the tone decoder occupancy threshold for calls under surveillance.

This threshold (specified as a percentage of the total number of tone decoders in the office) is used to control when tone decoders are dropped from surveillances where no digits have been collected for more than 1 minute.

NOTE: The TD LIMIT is only applicable when the DTMF STATUS field on view C.4 is set to STANDARD.

An example of view 8.1, screen 13, showing the new TD LIMIT field follows.

```
5ESS SWITCH
SCREEN 13 OF 15                        RECENT CHANGE  8.1
(5509)                        OFFICE PARAMETERS (MISCELLANEOUS)

227. ACCT PROMPT      _______     235. CALEA SM      _
228. CARRIER TONE     _           236. ADMIN ACCESS  _
229. NSC WC ID        ___         237. TD LIMIT      50
```

```
230. ORIG NSC        ___
231. TERM NSC        ___
232. TEST CALL TNSC  ___

    INCREASED TGN
233. MAX TGN    ____
234. MAX RTIDX  _____
```

3.7.2 PROCEDURE

(1) Activate a Recent Change session at a non-CALEA terminal.

Type and enter **RCV:MENU:APPRC;**

Response: A Recent Change session is started and the Main Menu appears.

(2) Access view 8.1 (in the update mode) by entering **8.1u**

Response: View 8.1 appears with the the cursor in the key field (**OFFICE ID**):

(3) Enter the office identifier in the key field, followed by a carriage return.

Response: View 8.1 appears with all currently-defined fields filled in.

(4) Change the tone decoder occupancy threshold by entering **C** (for the "change" operation) followed by a carriage return. At the Change Field prompt, enter **TD LIMIT** followed by a carriage return. The cursor is positioned at the TD LIMIT field. Enter a number from **0** — **90** (default = 50) (this number specifies the total number of tone decoders (as a percentage) that can be used simultaneously).

Response: Field **TD LIMIT** is changed.

(5) Type * or **U** to update the view in the database.

Response: **updating...**

followed by **FORM UPDATED**

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.8 CDC/PDC PROVISIONING

3.8.1 OVERVIEW

The Call Data Channel (CDC) is a SMP TCP socket connection (established during subject provisioning) between the *5ESS*® switch and the LEA monitoring station. Circuit and packet call-identifying information is collected by the Switching Module Processor (SMP) that is supporting the subject under surveillance and is formatted into CDC messages. Each SMP TCP connection is supported by an X.25 Permanent Virtual Circuit (PVC) to transport CDC messages from the *5ESS*® switch to the CALEA monitoring station.

In the 5E16.2 FR1 software release, 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 a lower cost alternative to using a SMP TCP socket connection.

The Packet Data Channel (PDC) is a pair of TCP socket connections between the *5ESS*® switch and the LEA monitoring station (collection facility). Each PDC TCP connection is supported by an X.25 Permanent Virtual Circuit (PVC) to transport packet call content from the *5ESS*® switch to the CALEA monitoring station.

See 235-190-104, *ISDN Feature Descriptions*, for information on X.25 provisioning.

NOTE 1: CALEA is supported on both National and Custom ISDN.

NOTE 2: To guard against loss of surveillance connectivity due to link failure, multiple INET Interfaces which are mapped to the same Destination IP address or subnet can be created via RC/*V* 33.3.

Multiple INET PVC Interfaces can be defined for different DEST IP ADDR (LEAs) using the same physical BRI(1 or 2 B-Channels)/T1 (1 to 24 DS0s) link (assuming IP Traffic considerations must be taken into account).

Multiple INET PVC Interfaces defined for the same DEST IP ADDR will result in load sharing between Interfaces (assuming the route metric for each Interface path is the same).

For 5E16.2 software release, with CDC Dial Out option, Switched Virtual Circuits (SVC) 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.

An 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.

SCVs are provisioned using the following RC/*V* screens:

- RC/*V* 23.40 (XAT) - used to support new PSUEN XAT (OE type = U).
- RC/*V* 33.2 - used to insert an IP interface used by CDC Dial Out TCP/IP sockets.
- RC/*V* 33.3 - used to provision similarly to existing PVC CDC case.

3.8.2 CDC/PDC INET PVC AND SVC PROVISIONING

3.8.2.1 BRI INET PVC PROVISIONING

CDC and PDC have similar growth procedures. To provision a BRI, use View 23.2 for provisioning an X.25 line, followed by view 23.11 to assign PVCs to DSLs.

NOTE: CALEA-specific RC/V field values are noted in text as well as in the view examples. Other values are for example only, and may be different for your provisioning depending on your switch's configuration. Views with multiple screens have only the CALEA-impacted screens exemplified.

View 23.2, DIGITAL SUBSCRIBER LINE

```
                                        5ESS SWITCH
SCREEN 1 OF 16                        RECENT CHANGE  23.2
(5900,5900A,5901)                  DIGITAL SUBSCRIBER LINE

(*)1. DSL TN _ __________          SERVICES
(*)4. MLHG    ____                 AND FEATURES    SCREENS
(*)5. TERM    ____                 ----------------------
(*)6. DSL OE _ __________          CKT              4 to 7
(*)9. ASSOC  _                     DPKT              8 & 9
                                   DSL INFO             2
                                   ISAT ICI            16
                                   ODB              10 & 11
                                   PPB1             12 & 13
                                   PPB2             14 & 15
                                   USER INFO            3
```

```
                                        5ESS SWITCH
SCREEN 12 OF 16                       RECENT CHANGE  23.2
(5900,5900A,5901)                DIGITAL SUBSCRIBER LINE (PPB1)

>309. PPB1 TN    __________        320. ISCN     ______   331. H PVC LCN   2
 310. LCC        ___               321. RATE     ____     332. L IN  LCN ___
 311. RAX        __                322. N2       __       333. H IN  LCN ___
 312. MLHG       ____              323. T1       ___      334. L 2W  LCN ___
 313. TERM       ____              324. T3       __       335. H 2W  LCN ___
 314. LNR HNT TN __________        325. WNDSZ    _        336. L OUT LCN ___
 315. HUNT DEACT _                 326. DPIDB    __       337. H OUT LCN ___
 316. CHL SEL    _                 327. TS       __       338. BUSY LIMIT ___
 317. NEW TN     __________        328. DS1      __       339. ICB _
 318. BILL TN    __________        329. DS1 TS   __       340. OCB _
 319. RMK        ________________                         341. PMDR GRP ________
                                                          342. PMDR ACT _
```

View 23.11, DSL PACKET SWITCHING PVC LCN ASSIGNMENT, is used to make all Permanent Virtual

Circuit assignments to digital subscriber lines, such as DPKT, ODB, PPB1 and PPB2.

NOTE: CDC and PDC BRI PVCs are supported on PPB1 or PPB2 only.

```
                                        5ESS SWITCH
                                      RECENT CHANGE  23.11
(5923)                      DSL PACKET SWITCHING PVC LCN ASSIGNMENT

(*)1. PKT TN       __________      13. REMOTE LCN  ____
(*)2. PKT MLHG     ____            14. REMOTE TN   __________
(*)3. PKT MEMB     ____            15. REMOTE DNIC ____
  *4. LCN          ___             16. PSN         ___
   5. SEND PKTSZ   ___             17. INTRA GROUP _
   6. SEND PKTWD   _
   7. RCV PKTSZ    ___
   8. RCV PKTWD    _
  #9. CALL IND     _______
  10. BILLABLE     _
 #11. FCL TYPE     ____
  12. LINK ID      ___
```

- A warning will be issued when FCL TYPE=INET and SEND/RCV PKTSZ=128 and SEND/RCV PKTWD=2 values are entered. The recommended values are SEND/RCV PKTSZ=256 and SEND/RCV PKTWD=7.
- When FCL TYPE=INET, LINK ID, REMOTE LCN, REMOTE TN, REMOTE DNIC, and PSN will be blank and CALL IND must be CALLING.
- There is a crosscheck between the SEND PKTSZ value on view 23.11 and the MTU SIZE value on view 33.2. MTU SIZE cannot be greater than SEND PKTSZ.

3.8.2.2 XAT INET PVC PROVISIONING

To provision an XAT, use view 23.40, X.25 (XAT) PACKET SWITCHING CHANNEL ASSIGNMENT, followed by view 23.11 to assign PVCs to DSLs.

```
                                        5ESS SWITCH
SCREEN 1 OF 3                         RECENT CHANGE  23.40
(5909,5909A,5909B)     X.25 (XAT) PACKET SWITCHING CHANNEL ASSIGNMENT

(*)1. PKT TN     __________             15. PKT NEW TN __________
(*)2. PKT MLHG   ____                   16. ISCN       ______
(*)3. TERM NBR   ____                  #17. LCC        ___
(*)4. OE         _ ___________         #18. RAX        __
          CHANGE FIELDS                 19. RATE       ____
```

```
  7. CHNG PKT TN   __________        20. N2          __
  8. CHNG PKT MLHG ____              21. T1          ___
  9. CHNG TERM NBR ____              22. T3          __
 10. CHNG OE       _ ___________     23. WNDSZ       _
       MLHG ONLY                     24. SUST        _
 13. LNR HNT TN   __________        25. BILL TN     __________
 14. HUNT DEACT   _                 26. RMK         ________________
```

```
                                        5ESS SWITCH
SCREEN 2 OF 3                          RECENT CHANGE  23.40
(5909,5909A,5909B)    X.25 (XAT) PACKET SWITCHING CHANNEL ASSIGNMENT

27. OCU LOOPBACK _       39. BUSY LIMIT ___          51. ICP         _
28. CSU LOOPBACK _       40. HUNT NOTIF ___          52. PB GRP      ___
29. X25VER       ____    41. PMDR GRP   ________     53. REV CHARGE  _
30. ICB          _       42. PMDR ACT   _            54. LCP         _
31. OCB          _       43. SEND TPC   _____        55. FCPN        _
32. H PVC LCN    ___     44. SEND PKTSZ ___          56. TPCN        _
33. L IN LCN     ___     45. SEND PKTWD _            57. FSA         _
34. H IN LCN     ___     46. SEND MCT   ___          58. IA          _
35. L 2W LCN     ___     47. RCV TPC    _____        59. IECP DNIC   ____
36. H 2W LCN     ___     48. RCV PKTSZ  ___
37. L OUT LCN    ___     49. RCV PKTWD  _
38. H OUT LCN    ___     50. RCV MCT    ___
```

View 23.11, DSL PACKET SWITCHING PVC LCN ASSIGNMENT, is used to make all Permanent Virtual Circuit assignments to digital subscriber lines, such as DPKT, ODB, PPB1 and PPB2. This view is also used to make PVC assignments for X.25 channels on a T1 (XATs).

NOTE: CDC and PDC BRI PVCs are supported on PPB1 or PPB2 only.

```
                                        5ESS SWITCH
                                       RECENT CHANGE  23.11
(5923)                        DSL PACKET SWITCHING PVC LCN ASSIGNMENT

(*)1. PKT TN      __________       13. REMOTE LCN  ____
(*)2. PKT MLHG    ____             14. REMOTE TN   __________
(*)3. PKT MEMB    ____             15. REMOTE DNIC ____
  *4. LCN         ___              16. PSN         ___
   5. SEND PKTSZ  ___              17. INTRA GROUP _
   6. SEND PKTWD  _
   7. RCV PKTSZ   ___
```

```
  8. RCV PKTWD   _
 #9. CALL IND    _______
 10. BILLABLE    _
#11. FCL TYPE    ____
 12. LINK ID     ___
```

- A warning will be issued when FCL TYPE=INET and SEND/RCV PKTSZ=128 and SEND/RCV PKTWD=2 values are entered. The recommended values are SEND/RCV PKTSZ=256 and SEND/RCV PKTWD=7.
- When FCL TYPE=INET, LINK ID, REMOTE LCN, REMOTE TN, REMOTE DNIC, and PSN will be blank and CALL IND must be CALLING.
- There is a crosscheck between the SEND PKTSZ value on view 23.11 and the MTU SIZE value on view 33.2. MTU SIZE cannot be greater than SEND PKTSZ.

3.8.2.3 XAT INET SVC PROVISIONING

The XAT PH channel group member (PSUEN) is provisioned to support X.25 SVCs using the outgoing LCN range, as specified on RC 23.40. The TCP/IP interface name is provisioned using a specific LCN from the outgoing LCN range. When a X.25 SVC is initiated, the LCN associated with the TCP/IP interface (gateway) used to reach the destination IP address (law enforcement collection facilities) is used along with the destination X.25 address from the provisioned CALEA (RCV C.4).

To provision an PSUEN XAT, use view 23.40, X.25 (XAT) PACKET SWITCHING CHANNEL ASSIGNMENT.

NOTE: RC/V 23.11 is **not** used for SVCs , only PVCs.

```
                                        5ESS SWITCH
SCREEN 1 OF 3                          RECENT CHANGE  23.40
(5909,5909A,5909B)    X.25 (XAT) PACKET SWITCHING CHANNEL ASSIGNMENT

(*)1. PKT TN     __________             15. PKT NEW TN __________
(*)2. PKT MLHG   ____                   16. ISCN       ______
(*)3. TERM NBR   ____                  #17. LCC        ___
(*)4. OE         _ __________          #18. RAX        __
         CHANGE FIELDS                  19. RATE       ____
   7. CHNG PKT TN   __________          20. N2         __
   8. CHNG PKT MLHG ____                21. T1         ___
   9. CHNG TERM NBR ____                22. T3         __
  10. CHNG OE       _ __________       23. WNDSZ      _
       MLHG ONLY                        24. SUST       _
  13. LNR HNT TN __________             25. BILL TN    __________
  14. HUNT DEACT _                      26. RMK        ________________
```

- OE type is U, for a newly supported PSUEN XAT.

```
                                    5ESS SWITCH
SCREEN 2 OF 3                     RECENT CHANGE  23.40
(5909,5909A,5909B)    X.25 (XAT) PACKET SWITCHING CHANNEL ASSIGNMENT

27. OCU LOOPBACK _       39. BUSY LIMIT ___          51. ICP         _
28. CSU LOOPBACK _       40. HUNT NOTIF ___          52. PB GRP      ___
29. X25VER       ____    41. PMDR GRP   ________     53. REV CHARGE  _
30. ICB          _       42. PMDR ACT   _            54. LCP         _
31. OCB          _       43. SEND TPC   _____        55. FCPN        _
32. H PVC LCN    ___     44. SEND PKTSZ ___          56. TPCN        _
33. L IN LCN     ___     45. SEND PKTWD _            57. FSA         _
34. H IN LCN     ___     46. SEND MCT   ___          58. IA          _
35. L 2W LCN     ___     47. RCV TPC    _____        59. IECP DNIC   ____
36. H 2W LCN     ___     48. RCV PKTSZ  ___
37. L OUT LCN    ___     49. RCV PKTWD  _
38. H OUT LCN    ___     50. RCV MCT    ___
```

The following values are recommended:

- Flow control and Throughput Control Negotiation is supported on the emulated DTE. As such, FCPN and TCPN should be set to "Y".
- SEND/RCV PKTSZ=256, SEND/RCV PKTWD=7, and SEND/RCV TCP=19200.
- The BRI/XAT/X.75/X.75' outgoing facilities must also support matching PKTSZ, PKTWD, and TPC values.
- The corresponding RC View 33.2 MTU Size should always be 128 (never set to 256).

NOTE: The X.25 input and output window size parameters of the terminating DTE (e.g., router) is recommended to be set to 2 so as to provide more frequent X.25 packet acknowledgements to the PSUEN XAT emulated DTE, thus improving throughput.

3.8.2.4 X.75/X.75' INET PVC PROVISIONING

It is assumed that an X.75/X.75' trunk group is already provisioned. If not, assign an X.75/X.75' trunk group using RC/V view 5.1.

View 5.5, TRUNK MEMBER, is used to define each member of a trunk group.

```
                                        5ESS SWITCH
SCREEN 1 OF 6                         RECENT CHANGE  5.5
(5204)                                  TRUNK MEMBER

  *1. TGN             660           23. HOLD BUSY     N
  *2. MEMB NBR        0             24. SATELLITE     N
(*)9. QTY             1             25. TRF SAMPLE    N
 #12. OE              D 00410125    26. CAMOPTLK TEN  _______
  15. CLCI TRK ID     ____          27. CAMOPTLK DEN  ________
  16. TRANS CLASS     2             28. CAMOPTLK NEN  ___________
  17. SUPV            EM2           29. ACTN          R
  18. IDLE STATE      ON            30. OTODPN1       _________
  19. IN START DIAL   NONE          31. OTODPN2       _________
  20. OUT START DIAL  NONE          32. SLC OTODPN3   _________
  21. STOPGO          N             33. SLC OTODPN4   _________
  22. CGA SPN         _________     34. MAXCALLS      __

Enter Review, Change-insert, Validate, screen#, or Print:
```

```
                                        5ESS SWITCH
SCREEN 3 OF 6                         RECENT CHANGE  5.5
(5204)                                  TRUNK MEMBER

   PACKET SWITCHING              PACKET SWITCHING X75/X75P
74. OCU LOOPBACK _    81. LINK ID                ___   88. HIGH PVC LCN ___
75. CSU LOOPBACK _    82. SEND THRUPUT CLASS     _____ 89. LCN HI TO LOW _
76. LAPB ADDR    _    83. RCV  THRUPUT CLASS     _____ 90. LOW INCOMING LCN ___
77. WINDOW SIZE  _    84. SEND PKT SIZE          ___   91. HI  INCOMING LCN ___
78. RETRANS N2   __   85. RCV  PKT SIZE          ___   92. LOW 2 WAY LCN ___
79. ACK TIME T1  ___  86. SEND PKT WINDOW SIZE   _     93. HI  2 WAY LCN ___
80. IDLE TIME T3 __   87. RCV  PKT WINDOW SIZE   _     94. LOW OUTGOING LCN ___
                                                      95. HI  OUTGOING LCN ___
```

View 5.13, TRUNK PACKET SWITCHING PVC LCN ASSIGNMENT, is used to provision permanent virtual circuits (PVCs) for X.75/X.75' packet trunks. This view, along with view 23.11, was modified to allow an FCL

TYPE of INET in order to use these PVCs for a CDC or PDC connection.

```
                                        5ESS SWITCH
                                      RECENT CHANGE  5.13
(5926)                    TRUNK PACKET SWITCHING PVC LCN ASSIGNMENT

*1. TGN          ____          10. SEND THRUPUT CLASS    _____
*2. MEMB         __            11. RCV THRUPUT CLASS     _____
*3. LCN          ___           12. SEND PKT SIZE         ___
#4. CALL IND     _______       13. RCV PKT SIZE          ___
#5. FCL TYPE     ____          14. SEND PKT WINDOW SIZE  _
 6. REMOTE LCN   ____          15. RCV PKT WINDOW SIZE   _
      X25 FCL TYPE
 7. REMOTE TN    __________              X75 TGN
                               16. PVC ID NUMBER ____
 X75P FCL TYPE                 17. BILLABLE      _
 8. LINK ID ___
 9. PSN     ___
```

- A warning will be issued when FCLTYPE=INET and SEND/RCV PKTSZ=128 and SEND/RCV PKTWD=2 values are entered. The recommended values are SEND/RCV PKTSZ=256 and SEDN/RCV PKTWD=7.
- When FCLTYPE=INET, LINK ID, REMOTE LCN, REMOTE TN, and PSN will be blank and CALL IND must be CALLING.
- There is a crosscheck between the SEND PKTSZ value on view 5.13 and the MTU SIZE value on view 33.2. MTU SIZE cannot be greater than SEND PKTSZ.

3.8.3 CDC ANALOG LINE TERMINATION PROVISIONING

In the 5E16.2 FR1 software release, the CALEA CDC with Voice Band Data Transmission feature (99-5E-8318) introduces the following provisioning issues for GR-30 CDC links (analog line interface):

(1) The GR-30 CDC Local DN must be an analog DN with caller ID with call waiting (or any other analog display feature) active on the line. It also must have the ability to use Direct Distance Dialing (DDD) dial plan

(2) The following features may be assigned and active on a line acting as a GR-30 CDC Destination DN for a GR-30 CDC Link:

- CFV (includes all variants of call forwarding variable: e.g., /CFV, /CFPF, /CFV1A, etc.)
- CFBL (includes all variants of call forwarding busy line: e.g., /CFBLAC, /CFBLFB, /CFIBL, etc.)
- CFDA (includes all variants of call forwarding don't answer a.k.a. CF No Reply: e.g., /CFDAAC,

/CFDAFB, /CFIDA, etc)

- CLASS Selective Call Forwarding (SCF) or Selective Call Acceptance (SCA) when rerouted to another directory number
- Series Completion
- Multi-Line Hunt Group (MLHG) without queuing
- Terminal Group and Station Restriction (TGSR) that is rerouted to another directory number

A line with any of the following features assigned and active will **NOT** be able to be used as a GR-30 CDC Destination DN for a GR-30 CDC link:

- Intraswitch MLHG queuing
- Call pickup (all variants)
- Call park (all variants)
- Redirections to intraswitch announcements (e.g., fixed route, TGSR, SCA, etc.)
- The LEA destination DN cannot be an operator-assisted (0+, 0-) or N11 DN
- Call waiting (all variants)

If the CB utilizes a device that uses dial-tone detection to determine disconnect, 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.

3.8.4 CDC/PDC IP ADDRESS PROVISIONING

A subject has at least one associated LEA monitoring station's IP address. Each LEA monitoring station has a unique IP address. An SM housing a circuit and/or packet-switched subject requires the creation of a socket or a pair of sockets respectively, from that SM to each LEA monitoring station with which the subject is associated.

A socket is a path that is defined by a pair of addresses, for example, the local internet protocol (IP) address and port number of the transmission control protocol (TCP), and the destination 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.

The socket between a SM and a monitoring station carries CDC information for all subjects in that SM that are associated with the monitoring station. Each packet-switched subject in a PH requires the creation of a pair of sockets from that PH to each monitoring station with which the subject is associated. One member of the socket pair will carry (PDC content) data sent by the subject and the other member will carry data received by the subject.

In 5E16.2 software release, the capability to set up and establish Switched Virtual Circuits (SVCs) for the Call Data Channel (CDC) TCP/IP Sockets is added. Currently, only Permanent Virtual Circuits (PVCs) are

supported for CALEA CDC TCP/IP Sockets. This feature adds the capability of supporting TCP/IP Sockets on SVCs originated by a PSUEN XAT PH channel group member for the CDCI component of the CALEA application.

Each SMP TCP connection is supported by an X.25/X.75/X.75' PVC and/or an X.25 SVC to transport CDC messages from the *5ESS*® switch to the CALEA monitoring station. Generally, a PVC is provisioned when a *5ESS*® switch is likely to have (several) on-going CALEA surveillances. Conversely, if few CALEA surveillances are expected on a switch, an XAT PH Channel Group Member (PSUEN) is provisioned to support SVCs on one or more Incoming Logical Channel Number (LCNs) to reduce the time and cost of establishing nailed up connections required for PVCs. An X.25/X.75/X.75' packet network is required for SVCs; however, an SMP TCP socket connection is established only when CDC messages are sent from a specific SM for an active surveillance. The first CDC message sent via a specific TCP interface (IP gateway) will establish the SVC using the X.25 destination address specified by the surveillance case and a LCN provisioned for the TCP interface. The TCP socket for the SMP attempting to send a CDC message is established after the SVC is established and routing internet protocol (RIP) messages initialize IP routing tables in the switch SMPs and PHs. The CDC messages are buffered until the SMP TCP socket is established to the destination CALEA monitoring station. Messages will be buffered until the buffer is full. Once full, the older CDC messages will be removed from the buffer and sent to the CALEA ROP.

NOTE: There is a limit of 3 surveillances per PH. A surveillance of one subject with 3 packet services on one PH is counted as 3 surveillances. It may be necessary to move subjects from one PH to another if the capacity for the PH has been exceeded.
In other words, 3 services x 2 PDC sockets/service x 5 LEAs equates to a total of 30 PDC sockets from the subject PH distributed across the 5 LEAs.
This limit applies to PH3 and PH4 Protocol Handlers with a DSL type (channel group type) of DSLG.

NOTE: Every SMP must have an IP address residing on the inter-SMP subnet. Refer to Figure 3-7 for a graphical representation of subnets.

NOTE: For Level 1 surveillances, ISMs are not used because the SM generates the CDC messages and sends them via sockets created in the SM. For Level 2 surveillances using a PDC connection, if the subject resides on the SM that contains the delivery PH, then a pair of ISMs is **not** needed. However, if the subject resides on an SM that does not contain the delivery PH, then an appropriate ISM pair (PH3 or PH4) is required between the subject's SM and the SM containing the delivery PH. ISMs are required for SVC CDC connections if the emulated DTE and outgoing BRI/XAT/X.25/X.75/X.74' facilities are not on the same SM.

In both CDC and PDC sockets, the *5ESS*® switch(es) is the client and the LEA monitoring stations are the servers. The servers listen for an incoming socket connection via a TCP port number that is made known in the *5ESS*® switch(es) via provisioning. Figure 3-6 provides an overview of the CALEA network.

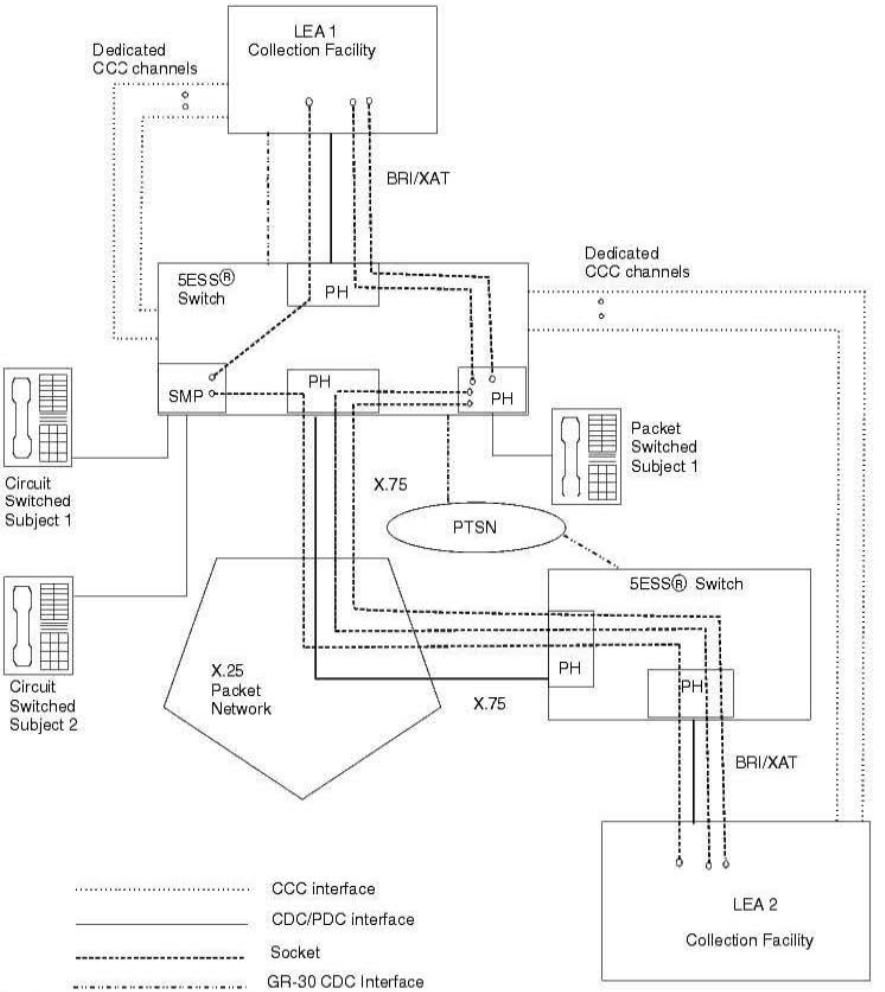


Figure 3-6 CDC/PDC Network Block Diagram

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 an SM and the second IP address assigned to

the SMP.

Figure 3-7 provides an example of IP address assignments in a switch.

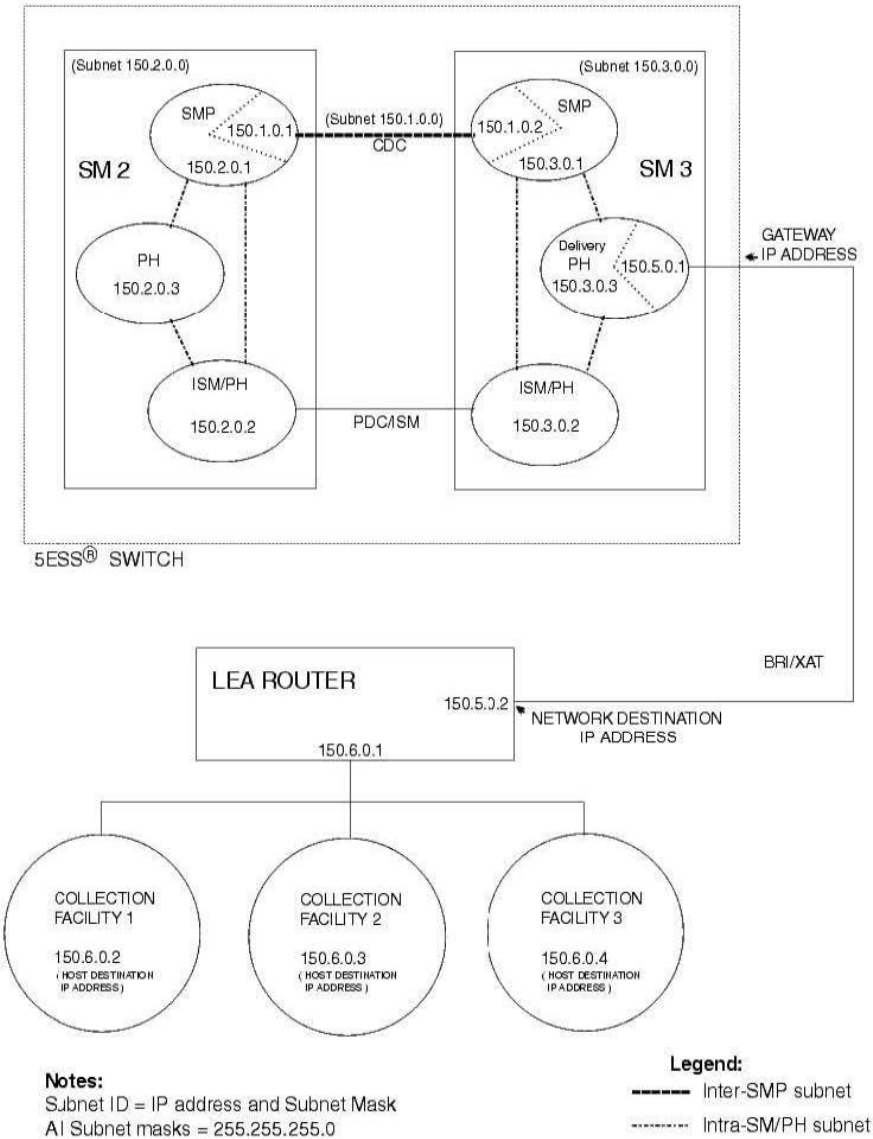


Figure 3-7 IP Address Assignment Example IP Address Assignment Example

View 33.1, INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT, is used to provision up to five IP addresses and subnet masks, and associated IP and TCP parameters to a processor (SM or PH). Each SMP can have multiple IP addresses internally so as to communicate with a subnet of SMPs as well as a subnet of PHs. Each PH has one IP address and belongs to the intra-SM/PH subnet. This subnet will include PHs as well as the second IP address assigned in the SMP.

NOTE: For a PH, the value for the QUALIFIER 2 field is the PSU community address (COM ADDR) found on recent change view 22.2. For an SM, leave the QUALIFIER 2 field blank. Please refer to Chapter 6 for a complete description of the view and its fields.

NOTE: The value for QUALIFIER 3 is three digits, representing the PSU shelf number (0-4) and the channel group number (00-15). For delivery PH, the value for the QUALIFIER 3 field is the first three digits of the "ISCN" field on the DIGITAL SUBSCRIBER LINE (PPB1) or (PPB2) screen of Recent Change view 23.2, or the first three digits of the "ISCN" field on Recent Change view 23.40, X.25 XAT PACKET SWITCHING CHANNEL ASSIGNMENT.

NOTE: IP addresses consist of a Network ID and Host ID. The Host ID should not consist of contiguous binary zeroes or contiguous binary ones. The Host ID is determined by performing a binary AND between the IP address and the complemented Subnet Mask. The contiguous binary ones in the complemented Subnet Mask determine the bit size length of the Host ID.

NOTE: When the first IP address of a particular subnet is inserted via 33.1, the route table of all previously configured SMPs and PHs will be updated stating whether connectivity to that subnet is possible from a particular SMP or PH.

Following are examples of the recent change screens showing various IP address assignments and which Recent Change views are used. The values shown correspond to the values in Figure 3-7 and are for example only.

SM 2 Processor IP Address Assignment Examples

First, SM 2's SMP IP addresses are assigned.

```
                                        5ESS SWITCH
SCREEN 1 OF 2                        RECENT CHANGE  33.1
(5987)                 INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

  *1. PROCESSOR ID    2
  *2. PROCESSOR TYPE SM
(*)3. QUALIFIER 2     ___
(*)4. QUALIFIER 3     ___

          5. IP ADDRESS
ROW LOCAL IP ADDR    IP SUBNET MASK
 1  150.001.000.001 255.255.255.000
 2  150.002.000.001 255.255.255.000
 3  ___.___.___.___ ___.___.___.___
 4  ___.___.___.___ ___.___.___.___
 5  ___.___.___.___ ___.___.___.___
```



```
                                          5ESS SWITCH
SCREEN 2 OF 2                           RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

IP PARAMETER ASSIGNMENT     UDP PARAMETER ASSIGNMENT
16. REASSEM TIMER 60        23. UDP CHKSUM EN  Y
17. ICMP ERR CNT  64        24. UDP START PORT 49152
18. MTU ENABLE    N         25. UDP DEF TTL    255
19. MTU DISC      30

TCP PARAMETER ASSIGNMENT
20. TCP MSS         256
21. TCP START PORT 49152
22. TCP DEF TTL    255
```

Second, SM 2's delivery PH IP address is assigned.

```
                                          5ESS SWITCH
SCREEN 1 OF 2                           RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

  *1. PROCESSOR ID   2
  *2. PROCESSOR TYPE PH
(*)3. QUALIFIER 2     _2
(*)4. QUALIFIER 3     001

          5. IP ADDRESS
ROW LOCAL IP ADDR   IP SUBNET MASK
 1  150.002.000.003 255.255.255.000
 2  ___.___.___.___ ___.___.___.___
 3  ___.___.___.___ ___.___.___.___
 4  ___.___.___.___ ___.___.___.___
 5  ___.___.___.___ ___.___.___.___
```

```
                                        5ESS SWITCH
SCREEN 2 OF 2                         RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

IP PARAMETER ASSIGNMENT     UDP PARAMETER ASSIGNMENT
16. REASSEM TIMER 60        23. UDP CHKSUM EN  Y
17. ICMP ERR CNT  64        24. UDP START PORT 49152
18. MTU ENABLE    N         25. UDP DEF TTL    255
19. MTU DISC      30

TCP PARAMETER ASSIGNMENT
20. TCP MSS         256
21. TCP START PORT 49152
22. TCP DEF TTL    255
```

Third, SM 2's ISM/PH IP address is assigned.

```
                                        5ESS SWITCH
SCREEN 1 OF 2                         RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

  *1. PROCESSOR ID   2
  *2. PROCESSOR TYPE PH
(*)3. QUALIFIER 2    _2
(*)4. QUALIFIER 3    005

          5. IP ADDRESS
ROW LOCAL IP ADDR   IP SUBNET MASK
 1  150.002.000.002 255.255.255.000
 2  ___.___.___.___ ___.___.___.___
 3  ___.___.___.___ ___.___.___.___
 4  ___.___.___.___ ___.___.___.___
 5  ___.___.___.___ ___.___.___.___
```

```
                                        5ESS SWITCH
SCREEN 2 OF 2                         RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

IP PARAMETER ASSIGNMENT     UDP PARAMETER ASSIGNMENT
```

```
16. REASSEM TIMER 60        23. UDP CHKSUM EN  Y
17. ICMP ERR CNT  64        24. UDP START PORT 49152
18. MTU ENABLE    N         25. UDP DEF TTL    255
19. MTU DISC      30

TCP PARAMETER ASSIGNMENT
20. TCP MSS         256
21. TCP START PORT 49152
22. TCP DEF TTL    255
```

SM 3 Processor IP Address Assignment Examples

First, SM 3's SMP IP address(es) are assigned.

```
                                        5ESS SWITCH
SCREEN 1 OF 2                         RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

  *1. PROCESSOR ID   3
  *2. PROCESSOR TYPE SM
(*)3. QUALIFIER 2    ___
(*)4. QUALIFIER 3    ___

          5. IP ADDRESS
ROW LOCAL IP ADDR   IP SUBNET MASK
 1  150.001.000.002 255.255.255.000
 2  150.003.000.001 255.255.255.000
 3  ___.___.___.___ ___.___.___.___
 4  ___.___.___.___ ___.___.___.___
 5  ___.___.___.___ ___.___.___.___
```

```
                                        5ESS SWITCH
SCREEN 2 OF 2                         RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

IP PARAMETER ASSIGNMENT     UDP PARAMETER ASSIGNMENT
16. REASSEM TIMER 60        23. UDP CHKSUM EN  Y
17. ICMP ERR CNT  64        24. UDP START PORT 49152
18. MTU ENABLE    N         25. UDP DEF TTL    255
19. MTU DISC      30
```

```
TCP PARAMETER ASSIGNMENT
20. TCP MSS         256
21. TCP START PORT 49152
22. TCP DEF TTL    255
```

Second, SM 3's delivery PH IP address is assigned.

```
                                        5ESS SWITCH
SCREEN 1 OF 2                         RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

  *1. PROCESSOR ID   3
  *2. PROCESSOR TYPE PH
(*)3. QUALIFIER 2    _3
(*)4. QUALIFIER 3    001

          5. IP ADDRESS
ROW LOCAL IP ADDR   IP SUBNET MASK
 1  150.003.000.003 255.255.255.000
 2  ___.___.___.___ ___.___.___.___
 3  ___.___.___.___ ___.___.___.___
 4  ___.___.___.___ ___.___.___.___
 5  ___.___.___.___ ___.___.___.___
```

```
                                        5ESS SWITCH
SCREEN 2 OF 2                         RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

IP PARAMETER ASSIGNMENT     UDP PARAMETER ASSIGNMENT
16. REASSEM TIMER 60        23. UDP CHKSUM EN  Y
17. ICMP ERR CNT  64        24. UDP START PORT 49152
18. MTU ENABLE    N         25. UDP DEF TTL    255
19. MTU DISC      30

TCP PARAMETER ASSIGNMENT
20. TCP MSS         256
21. TCP START PORT 49152
22. TCP DEF TTL    255
```

Third, SM 3's ISM/PH IP address is assigned.

```
                                        5ESS SWITCH
SCREEN 1 OF 2                         RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

  *1. PROCESSOR ID   3
  *2. PROCESSOR TYPE PH
(*)3. QUALIFIER 2    _3
(*)4. QUALIFIER 3    004

           5. IP ADDRESS
ROW LOCAL IP ADDR   IP SUBNET MASK
 1  150.003.000.002 255.255.255.000
 2  ___.___.___.___ ___.___.___.___
 3  ___.___.___.___ ___.___.___.___
 4  ___.___.___.___ ___.___.___.___
 5  ___.___.___.___ ___.___.___.___
```

```
                                        5ESS SWITCH
SCREEN 2 OF 2                         RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

IP PARAMETER ASSIGNMENT     UDP PARAMETER ASSIGNMENT
16. REASSEM TIMER 60        23. UDP CHKSUM EN  Y
17. ICMP ERR CNT  64        24. UDP START PORT 49152
18. MTU ENABLE    N         25. UDP DEF TTL    255
19. MTU DISC      30

TCP PARAMETER ASSIGNMENT
20. TCP MSS         256
21. TCP START PORT 49152
22. TCP DEF TTL    255
```

View 33.2, INTERNET PROTOCOL (IP) INTERFACE ASSIGNMENT, is used to provision up to five IP addresses and subnet masks, and associated IP parameters to an internet (CALEA DSL) interface. For

CALEA, this view is used to link an IP address to a DSL interface. Normally each Delivery PH will have only one IP address and corresponding subnet tied to an interface name. Even though five IP addresses and subnets can be entered, only one will be used.

In 5E16.2 software release, the IP interface is assigned on RC/V 33.2. An update of a PSUEN XAT PH channel group member's X.25 Outgoing LCN range that conflicts with the LCN assigned to the IP interface associated with the PSUEN XAT PH channel group member results in a deletion of the corresponding IP interface assignments on RC/V 33.2.

NOTE: Do **not** delete or change the OE (PSUEN) of an XAT PH channel group member whenever one or more of the TCP/IP X.25 SVCs (LCNs) are marked with the (RC 33.2) CALEA USE set to YES unless the CALEA parameter, ALLOW CHNG, is set to YES.

NOTE: Do not set MTU SIZE for TCP/IP X.25 SVC LCNs to a value greater than 128.

The values shown correspond to the values in Figure 3-7 and are for example only.

Switch to LEA Interface IP Address Assignment Example

```
                                    5ESS SWITCH
                                  RECENT CHANGE  33.2
(5988)              INTERNET PROTOCOL (IP) INTERFACE ASSIGNMENT

(*)1. PKT TN          3132227759                    12. IP ADDRESS
(*)2. PKT MLHG        ____                    ROW GATEWAY IP ADDR IP SUBNET MASK
(*)3. PKT MEMB        ____                     1  150.005.000.001 255.255.255.000
(*)4. TGN             ____                     2  ___.___.___.___ ___.___.___.___
(*)5. TGN MEMB        __                       3  ___.___.___.___ ___.___.___.___
(*)6. OE              _ ____________           4  ___.___.___.___ ___.___.___.___
(*)9. ISCN            ______                   5  ___.___.___.___ ___.___.___.___
 *10. LCN             1
 #11. INTERFACE NAME  CALEA_BRI-1             23. MCAST ADDR   ___.___.___.___
                                              28. MTU SIZE     256
                                              29. CALEA IN USE N
```

View 33.3, INTERNET PROTOCOL (IP) ROUTING TO INTERFACE, is used to provision an IP gateway between an external IP destination on a LEA collection box and a local IP interface. For CALEA, this view is used to link LEA destination IP addresses with a gateway PH interface.

Information on view 33.3 is used to route IP datagrams off switch. The DEST IP ADDR and IP SUBNET MASK can either point to an individual host or can refer to an network of nodes in an IP subnet. Once an SM has a gateway IP address assigned to it using this view, all the SMPs and PHs configured via RC/V 33.1 will automatically be updated with the destination IP and Subnet Mask and corresponding gateway IP address.

In 5E16.2 software relase, the IP routing to interface is assigned on RC/V 33.3. An update of a PSUEN XAT PH channel group member's X.25 Outgoing LCN range that conflicts with the LCN assigned to the IP

interface associated with the PSUEN XAT PH channel group member results in a deletion of the corresponding IP routing to interface assignments on RC/V 33.3.

The values shown correspond to the values in Figure 3-7 and are for example only.

"NET" Destination Interface IP Address Assignments

```
                                        5ESS SWITCH
                                      RECENT CHANGE  33.3
(5989)                 INTERNET PROTOCOL (IP) ROUTING TO INTERFACE

 *1. DEST IP ADDR     150.006.000.000
 *6. INTERFACE NAME   CALEA_BRI-1
  7. NET OR HOST      NET
 #8. IP SUBNET MASK   255.255.255.000
#13. GATEWAY IP ADDR  150.005.000.001
 18. ROUTE METRIC     1
```

NOTE: Setting the DEST IP ADDR field to **150.006.000.000** sends messages to all collection facilities in that network (see Figure 3-7).

"HOST" Destination Interface IP Address Assignments

```
                                        5ESS SWITCH
                                      RECENT CHANGE  33.3
(5989)                 INTERNET PROTOCOL (IP) ROUTING TO INTERFACE

 *1. DEST IP ADDR     150.005.000.002
 *6. INTERFACE NAME   CALEA_BRI-1
  7. NET OR HOST      HOST
 #8. IP SUBNET MASK   ___.___.___.___
#13. GATEWAY IP ADDR  150.005.000.001
 18. ROUTE METRIC     1
```

NOTE: Setting the DEST IP ADDR field to **150.005.000.002** and the NET OR HOST field to **HOST** sends the messages to the "host" only (see Figure 3-7). The host then assumes responsibility for routing the messages to the LEAs networked to it; unless, however, the host is itself the LEA collection facility.

3.8.5 PROCEDURE FOR VERIFYING IP ADDRESS CONNECTIONS

3.8.5.1 PURPOSE

Execute the PING command to verify the connection established between the LEA and the switch. The PING command is also used to check all PH and SMP IP addresses assigned within the *5ESS*® switch from either the SMP subnet or the PH subnet.

3.8.5.2 PLANNING

The PING command can be executed any time a switch-to-LEA connection needs to be checked (for example, a new IP address has been assigned to a law enforcement agency collection facility). Refer to the command and report manual pages in Chapter 6 for complete details on command line options.

3.8.5.3 LIMITATIONS

The following two limitations apply to this procedure:

(1) Ping cannot be executed between IP addresses on the same SM.

(2) A Gateway IP address (found on RC/*V* view 33.2) cannot be pinged.

3.8.5.4 REQUIRED CONDITIONS AND TOOLS

The IP address of the destination to be "pinged" must be known. The PING command may be executed from any terminal allowing input commands.

3.8.5.5 PROCEDURE

NOTE: The equipment numbers and IP addresses used in this procedure are for example only. Refer to the command and report manual pages in Chapter 6 for complete details on command line options.

(1) Type **exc:ping,chng=20-0-0-10,ipdest=172-17-100-32;**

Response: PF (printout follows)
A successful ping will result in a report such as:

```
M  EXC PING REPLY FROM CHNG=20-0-0-10
     PH IMAGE TYPE = PH3 ISDN IMAGE
     SOURCE IP = 172.16.2.1
     DESTINATION IP = 172.17.100.32
     BYTES SENT = 126
     TIMEOUT = 5
     PING TIME     STATUS
     1     140     PING SUCCESS
     2     91      PING SUCCESS
```



```
3    91      PING SUCCESS
```

A timed-out ping will result in a report such as:

```
M  EXC PING REPLY FROM CHNG=20-0-0-10
     PH IMAGE TYPE = PH3 ISDN IMAGE
     SOURCE IP = 172.16.2.1
     DESTINATION IP = 172.17.100.32
     BYTES SENT = 126
     TIMEOUT = 5
     PING TIME    STATUS
     1    5002    PING TIMEOUT
     2    5099    PING TIMEOUT
     3    5098    PING TIMEOUT
```

(2) If the PING was unsuccessful, then check the IP address and retry the ping command. If the destination IP address is correct, then there may be a network problem with the destination machine. Also, try "pinging" portions of the network. For example, try pinging from an SMP to a delivery PH, from a delivery PH to a router, and from a router to a LEA collection box.

If the PING was successful, then this procedure is complete.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.8.6 PROCEDURE FOR VERIFYING IP ROUTE TABLE ENTRIES

3.8.6.1 PURPOSE

This procedure is used to verify the routes in the PNiproute table on a given switching module (SM) or channel group (CHNG).

3.8.6.2 PLANNING

The OP:TCPIP:RTDMP command can be executed any time an IP route entry needs to be checked (for example, after a recent change addition, change, or delete). Refer to the command and report manual pages in Chapter 6 for complete details on command line options.

3.8.6.3 REQUIRED CONDITIONS AND TOOLS

The OP:TCPIP:RTDMP command may be executed from any terminal allowing input commands.

3.8.6.4 PROCEDURE

NOTE: The equipment numbers and IP addresses used in this procedure are for example only. Refer to the command and report manual pages in Chapter 6 for complete details on command line options.

NOTE: Route Metrics of 1 to 15 are reachable whereas a route metric of 16 is considered unreachable.

NOTE: The basic usage of OP:TCPIP:RTDMP is to determine if the SMP or PH is capable of reaching the destination IP address or Subnet. One would do this by verifying that the destination is found as a route entry with a reachable Route Metric for every SMP and PH along the socket path through the

switch.

(1) Type **op:tcpip:rtdmp,sm=2;**

Response: PF (printout follows)
A successful route dump will result in a report such as:

```
M  OP TCPIP RTDMP ROUTE TABLE DUMP FOR SM=2  PAGE 1 OF 1
     PH IMAGE TYPE = NULL IMAGE

     ROUTE       DESTINATION      DESTINATION      GATEWAY
     NUMBER      IP ADDR          IP MASK          IP ADDR
     0           172.16.32.0      255.255.255.0    172.16.32.
     1           172.16.1.0       255.255.255.0    172.16.1.1
     2           172.16.3.0       255.255.255.0    172.16.32.3
     6           172.16.2.0       255.255.255.0    172.16.32.2

     ROUTE       INTERFACE        NEXT ROUTE       PREVIOUS
     METRIC      NUMBER           PTR              ROUTE PTR
     1           0                H'ffffffff       H'ffffffff
     1           1                H'ffffffff       H'ffffffff
     2           0                H'ffffffff       H'ffffffff
     2           0                H'ffffffff       H'ffffffff
```

(2) Unsuccessful system responses include NG and NO.

NG means "No good." The message was not accepted because the SM is isolated or the equipment does not exist. Check the equipment number in the input command and retry the input command.

NO is output when the feature not available. The requested action failed because the feature required to process the request is not present in the module.

If the route dump was successful, inspect the output. Based on the output, if more changes are required to the route table, then add, delete, or change routes via recent change. Re-execute this procedure to verify any additional changes made to the routing table. If the information is as expected, then this procedure is complete.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.8.7 LOCKING DOWN CALEA

Once an IP interface has been configured correctly on views 33.2 and 33.3, the CALEA IN USE field on view 33.2 can be set to "Y". This blocks certain recent change actions which could cause a surveillance to fail, such as deleting the PVC, or moving the OE to another SM. Surveillance-impacting recent change attempts result in a warning message alerting the switch personnel of the impact.

For surveillance-impacting recent changes to be done, the *5ESS*® switch Administrator must contact the Surveillance Administrator, who then unblocks Recent Change activity. The switch administrator then sets the CALEA IN USE field to "N", makes the necessary changes, then sets the CALEA IN USE field back to "Y". Once the switch administrator has completed the necessary changes, the Surveillance Administrator again changes a Recent Change field to block further surveillance-impacting recent changes.

3.8.8 PROCEDURE FOR TURNING OFF THE TPKT HEADER

3.8.8.1 PURPOSE

This procedure is used to exclude the TPKT header when transmitting CDC messages. Transmission of PDC message remains unchanged.

The TPKT header is required for PDC messages because it is the only indicator of the size of the X.25 packet to follow, but is redundant for CDC messages because the ASN.1 encoded also provides a length indication. Some LEA collection facilities cannot interpret the CDC message's TPKT information and require that the TPKT information be removed for CDC messages. Option feature ID 985 provides that capability.

3.8.8.2 PLANNING

By default, the TPKT header is included in all CDC messages. Prior to activating this feature, verify that all LEA collection facilities interfacing with the office are operating correctly. Contact your office's Surveillance Administrator, requesting that the OP:CDCTEST command be executed for each LEA collection facility linked to the office before executing this procedure.

Once the Option ID is activated, contact your office's Surveillance Administrator, requesting that the OP:CDCTEST command be executed again for each LEA collection facility linked to ensure that the interface is still working properly and that there are no CDC message errors.

3.8.8.3 REQUIRED CONDITIONS

The switch must be running a 5E14 or 5E15 software release with the CALEA-Core feature software.

3.8.8.4 REQUIRED TOOLS

A non-CALEA Recent Change terminal is required for accessing the general Recent Change database.

3.8.8.5 PROCEDURE

(1) Via the RC/V terminal, access view 8.31, OPTIONED FEATURES.

(2) Enter 'u' for update mode.

(3) Populate the following fields:

FIELD	VALUES
FEATURE ID	985
MODULE	OFC
ACTIVE	Y

Leave all remaining fields blank.

(4) Enter 'u' to update the form.

(5) Notify the Surveillance Administrator that this procedure has been completed and that the OP:CDCTEST command needs to be executed again for each LEA collection facility connected to the office.

If any of the Surveillance Administrator's OP:CDCTEST commands return with CDC message errors,

then Option ID 985 must be turned off by changing the "ACTIVE" field back to "N".

3.8.9 PROCEDURE FOR ACTIVATING AND DEACTIVATING CALEA SECURITY ENHANCEMENT

3.8.9.1 PURPOSE

This procedure is used to activate/de-activate the CALEA Security Enhancement which provides an extra layer of security which will prevent intentional or unintentional excessive TCP/IP datagrams/messages from adversely affecting the *5ESS*® switch performance.

If the LEA managed TCP/IP network elements are breached because of a flood of messages to the *5ESS*® switch via the Call Data Channel (CDC)/Packet Data Channel (PDC) Permanent Packet B-channel (PPB) can disrupt the operation of the *5ESS*® switch. Each message received over the CDC/PDC channel requires switch resources on the SM and PH to be used. If these messages arrive at an excessive or unexpected rate, a larger than normal amount of resources will be used to process these messages thus leaving fewer resources for other switch activities.

3.8.9.2 RESOLUTION and ENHANCEMENTS

With SFID 628 and OFID 708 active, the switch will operate as follows:

When an IP datagram is received from an external interface used by CALEA feature, the IP datagram shall be ignored unless it meets the following criteria:

- The source IP address of the received datagram must have a defined external return route (such as, be defined on RCV 33.3 [IP Routing to Interface]).

- The IP datagram is not a datagram fragment.

- The external interface PVC is used for CALEA (RCV 33.2 [IP Interface Assignment] field CALEA IN USE is Yes).

If the arrival rate of the IP datagram is more than 5 datagrams per 10 second period, the received IP datagram is ignored unless one of the following criteria is meet:

- The IP datagram TCP segment has no data and the CODE BITS in the TCP header are set as one of the following:
  * ACK
  * FIN
  * RST
  * SYN + ACK
  * FIN + ACK
- The IP datagram contains an ICMP message that is neither an ECHO REQUEST nor ECHO REPLY.

When an IP datagram is determined to be ignored, the following actions will be taken:

- The "ignored" IP datagram is dropped at the IP interface PH where it was received.
- On the CALEA SAS ROP, a CALEA SAS ERROR is logged with ERROR


```
      TYPE of one of the following:
      * Invalid IP route
      * IP datagram fragment received
      * Too many IP datagrams received
  - The IP interface's X.25 PVC within an HDLC channel will be
    reported as "overrun".  The "overrun" threshold is 3 within
    5 minutes.  Upon exceeding the threshold, the channel is
    automatically removed from service and automatically restored to
    service within 5 minutes.  While the PVC is OOS, any CDC or PDC
    message will be dropped due to the socket being OOS.
```

3.8.9.3 REQUIRED CONDITIONS

```
- SFID 509 (CALEA) is active in the office (RCV 8.22)

- IP interface is assigned and active (RCV 33.2 IP Interface
  Assignment field CALEA IN USE is Y)

- IP interface resides on a PH (Protocol Handler) with image
  PH3C, PH4A, or PH4G.

- SFID 628 has been purchased and activated.
```

3.8.9.4 PROCEDURE

To activate the CALEA Security Enhancement:

(1) Via the RC/V terminal, access view 8.31, OPTIONED FEATURES.

(2) Enter u for update mode.

(3) Populate the following fields:

FIELD	VALUES
FEATURE ID	708
MODULE	OFC
ACTIVE	Y

Leave all remaining fields blank.

(4) Enter u to update the form.

To deactivate the CALEA Security Enhancement:

(1) Via the RC/V terminal, access view 8.31, OPTIONED FEATURES.

(2) Enter u for update mode.

(3) Populate the following fields:

FIELD	VALUES
FEATURE ID	708
MODULE	OFC

ACTIVE	N

Leave all remaining fields blank.

(4) Enter u to update the form.

STOP. YOU HAVE COMPLETED THIS PROCEDURE.

3.9 CCC PROVISIONING

3.9.1 OVERVIEW

The CCC trunks (supported with a DFI-XT, DFI-2XT, DNU-S, or OIU) are outgoing digital trunks using no signaling. All CCCs must be provisioned on a single SM (the "delivery" SM). Local trunk hunting will be used for all CCCs so that the route request does not have to go to the CMP for processing. Call Content Channels (CCCs) are used to deliver call content from the subject's switch or Intercept Access Point (IAP) to up to 5 Law Enforcement Agencies (LEA). A CCC dedicated trunk circuit pair has only one intercept subject assigned to it. All trunk circuits within a CCC trunk group must terminate to the same LEA collection facility. The transmission characteristics and encoding for each CCC circuit conform to the applicable requirements in TR-NWT-000507, LSSGR Section 7 Transmission. CCC trunks always apply OdB loss to maintain data integrity for circuit-switched data calls. This is acceptable for circuit-switched voice calls because there is no echo path.

For a given surveillance, call content will be delivered over dedicated CCC pairs. Dedicated channels are connections that are permanently connected and 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 only the separated CCC option where separate channels are used for transmit and receive circuit-switched call content.

Each time that a call content channel is assigned to deliver call content, a message indicating channel identities for the transmit and receive call content is be sent to law enforcement. C-Tone (implemented as a single frequency tone of 480 Hz) may be is applied to a CCC channel when assigned to a surveillance but not connected to an active call. C-Tone is provisioned as either HIGHTONE or NULL (silence) by the Surveillance Administrator in the office, therefore the C-Tone provisioning procedure is outside the scope of this information product. HIGHTONE is not necessary for a surveillance to function.

The trunk class code used for CCCs is PF (Private Facility trunks) with a UCD hunt type. Trunks used to carry call content are the standard DNU/DFI/OIU digital trunks with time multiplexed signals complying with the digital formats given in ANSI T1.107-1988 and the electrical interface shall comply with ANSI T1.102-1987.

NOTE: It is recommended that CCC trunks be clear channel 64kb if ISDN subscriber services are provided by the office.

NOTE: The addition or removal of CCC trunks from a surveillance is not the same as adding or removing trunks from a *5ESS*® switch. Any assignment or unassingment does not change the physical connection to the LEA.

In 5E16 software release, for DialOut 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 an SS7 or MF trunk over the public switched telephone network. In both cases, the CCC connection will not be established

until the subject call is intercepted by answering the Destination LEA DN(s). The following CCC delivery modes are supported:

- **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.
- **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.

Instead of provisioning a CALEA TG on RC/V 5.1, an anlog line is provisioning (local LEA DN) with Remote Call Forwarding (RFC) active to an INVALID DN, such as 0, so direct calls to the line are not forwarded.

CALEA CCC trunks are provisioned as follows:

(1) Select the Delivery SM (view 8.1).

(2) Assign new CALEA trunk group with a trunk class of "PF" and a hunt type of UCD. (view 5.1)

(3) Define CALEA trunk members (view 5.5).

NOTE: For Digital Line Trunk Unit (DLTU), Digital Facilities Interface (DFI), Optical Interface Unit (OIU), and Digital Network Unit, the standard procedures shall be followed.

3.9.2 PREREQUISITE CONDITIONS

The prerequisites should have been performed in this order:

(1) The CALEA SFID (509) must be activated via Recent Change view 8.22 (NAR non-U.S./U.S. territories only).

(2) The Surveillance Administrator must have set the FEATURE ACTIVE field to 'Y' and the CTONE field to either 'HIGHTONE' or 'NULL' on Recent Change view C.1.

NOTE: Only the Surveillance Administrator has access to the "C" class of views.

3.9.3 SELECT DELIVERY SM

One SM needs to be specified as a "delivery" SM. Using view 8.1, OFFICE PARAMETERS (MISCELLANEOUS), define the SM number to be used as the delivery SM.

```
                                        5ESS SWITCH
SCREEN 13 OF 15                       RECENT CHANGE  8.1
(5509)                      OFFICE PARAMETERS (MISCELLANEOUS)

227. ACCT PROMPT      _______     235. CALEA SM  4
```

```
228. CARRIER TONE    _          236. ADMIN ACCESS N
229. NSC WC ID       ___        237. TD LIMIT     50
230. ORIG NSC        ___
231. TERM NSC        ___
232. TEST CALL TNSC  ___

    INCREASED TGN
233. MAX TGN     ____
234. MAX RTIDX   _____
```

3.9.4 PROVISION CALEA TRUNK GROUP

The following fields on view 5.1 must be populated as:

TRK DIR must be **OUTGO**

HUNT TYPE must be **UCD** or **LGUCD**

OUTPLS must be **NOSIGNAL**

INPLS must be **NOSIGNAL**

DCS TRK must be **N**

ATTTN must be **0**

TRKCLASS must be **PF**

MODULE must be equal to **CALEA SM** on view 8.1.

NOTE: The SM specified on view 8.1 will be cross-checked with the MODULE field on view 5.1.

CALEA must be **Y**

NOTE: A CALEA trunk group cannot have both CALEA and non-CALEA members. If yes ("Y"), then all trunk members in that trunk group are for CALEA use. If no ("N"), then the trunk and its members are not for CALEA use.

NOTE: A trunk group defined as a CALEA trunk group ("Y") can not be changed to a non-CALEA trunk group. In other words, the CALEA field can not be updated from "Y" to "N"). The insert and delete operations must be used to create and remove CALEA trunk groups. A CALEA trunk group can not be deleted while trunk members are assigned to that group.

```
                                        5ESS SWITCH
SCREEN 1 OF 13                        RECENT CHANGE  5.1
(5200,5202,5213)                        TRUNK GROUP
```

```
(*)1. TGN          660              13. CARRIER ID  ____      25. BRCS     N
(*)2. TRUNK CHAR   ________________ 14. FEAT GRP   _         26. FREE ANS N
(*)3. FEND CLLI    ___________      15. INC TND WNK N         27. PRIVACY  N
   4. TRK CHAR     ________________ 16. ATTTN       0         28. INSEP    0
   5. FAR CLLI     ___________      17. TERA RCVY   RPT       29. MODULE   4
   6. RMK          CALEA            18. IAPT        Y
  #7. TRK DIR      OUTGO            19. CALLMON INH Y             VERIFY ONLY
  #8. HUNT TYPE    UCD              20. INPLS       NOSIGNAL      GRP SIZ   8
   9. SCR          0                21. OUTPLS      NOSIGNAL      ACT SIZ   8
  10. GLARE ACTION ________         22. FAR END NPA 816           SATELLITE N
  11. DAS          0                23. GL ANN TGN  0             TERM SFG  N
 #12. TRK CLASS    PF               24. PBX/CPE ID  0

Enter Insert, Change, Validate, screen#, or Print:
```

```
                                        5ESS SWITCH
SCREEN 5 OF 13                        RECENT CHANGE  5.1
(5200,5202,5213)                        TRUNK GROUP

    NUMBER PORTABILITY                CELLULAR DATA
112. LRN DAS          __          120. DCS TRK    N
113. SIG PNUM         _           121. DCS RETRY  _
114. CNA OPTION       ______      122. DCS DIGCNT __
115. PORTED-IN AMA    _           123. CONT TEST  _
                                  124. SERV TYPE  ______
      DSN TRUNKS                       DCS NOTIFY _
116. DSN ARC ID __                126. ISG        _
117. SHCHECK    _                 127. ICOS TRK   _
118. MLPP STAGE ______            128. FAR E911   _

119. RTCD REQ _

Enter Insert, Change, Validate, screen#, or Print:
```

```
                                        5ESS SWITCH
SCREEN 12 OF 13                       RECENT CHANGE  5.1
```

```
(5200,5202,5213)                        TRUNK GROUP

241. API CODE ____                    END OFFICE NODAL
     MISCELLANEOUS              248. EON BILLING DN __________
242. EON MC RI      _____       249. EON NBR PLAN    ____
243. RERTE Q INH    N           250. EON PRIVACY     N
244. CALEA          Y           251. EON PREFIX NPA  N
245. REL LINK INIT  N           252. CNA MOD 164     N
246. SS7 ISUP OPER  N
247. SEND LD CIC    N




Enter Insert, Change, Validate, screen#, or Print:
```

NOTE: CALEA trunks must be restored to service, by executing the RST:TRK command, prior to any surveillances being assigned. RST:TRK can be used to restore individual trunks, a range of trunk members in a group, or a complete trunk group.

3.9.5 PROVISION CALEA TRUNK MEMBERS

After assigning trunk groups on view 5.1, TRUNK GROUP, use view 5.5, TRUNK MEMBER, to define each member of a trunk group.

CONDITIONS:

TGN must specify a trunk group which has **CALEA** set to **Y**.

OUT START DIAL must be blank or **NULL**.

OE for all CCCs (must be assigned to DFI, DNU-S, or OIU equipment) should be on the Delivery SM.

An even number of trunk members must be maintained.

CCCs for a specific case must be allocated in one contiguous block, therefore space between blocks of CCCs should be maintained to allow for future growth.

When a trunk is created in a CALEA trunk group, the **CALEA STATE** field will be set to **CRES**. Once the trunk member is assigned to a case by the Surveillance Administrator, the **CALEA STATE** field is set to **CTONE**. A trunk member that has CALEA status of CTONE (C-Tone applied) cannot be deleted. CTONE indicates that there is an active surveillance on this trunk member.

```
SCREEN 1 OF 6                          RECENT CHANGE  5.5
(5204)                                   TRUNK MEMBER

  *1. TGN             660           23. HOLD BUSY     N
  *2. MEMB NBR        0             24. SATELLITE     N
(*)9. QTY             1             25. TRF SAMPLE    N
 #12. OE              D 00410125    26. CAMOPTLK TEN  _______
  15. CLCI TRK ID     ____          27. CAMOPTLK DEN  ________
  16. TRANS CLASS     2             28. CAMOPTLK NEN  ___________
  17. SUPV            EM2           29. ACTN          R
  18. IDLE STATE      ON            30. OTODPN1       _________
  19. IN START DIAL   NONE          31. OTODPN2       _________
  20. OUT START DIAL  NONE          32. SLC OTODPN3   _________
  21. STOPGO          N             33. SLC OTODPN4   _________
  22. CGA SPN         _________     34. MAXCALLS      __

Enter Review, Change-insert, Validate, screen#, or Print:
```

```
                                         5ESS SWITCH
SCREEN 5 OF 6                          RECENT CHANGE  5.5
(5204)                                   TRUNK MEMBER

                   PACKET SWITCHING X75 ONLY UTILITY INDICATORS
121. TDI BEFORE    _  127. IN RPOA BEFORE  _  133. TNIC CONFIG  ______
122. TDI AFTER     _  128. IN RPOA AFTER   _  134. X75 ID  ___________
123. TDS BEFORE    _  129. OUT RPOA BEFORE _
124. TDS AFTER     _  130. OUT RPOA AFTER  _
125. TARIFF BEFORE _  131. RPOA DEL SEND   _
126. TARIFF AFTER  _  132. RPOA DEL RCV    _

   EEC OPTION         CALEA
     EEC ACTIVE _       CALEA STATE CRES
```

NOTE: CALEA trunks must be restored to service, by executing the RST:TRK command, prior to any surveillances being assigned. RST:TRK can be used to restore individual trunks, a range of trunk members in a group, or a complete trunk group.

3.9.6 FLOW DIAGRAMS - ADDING/DELETING A TRUNK GROUP AND MEMBERS

3.9.6.1 ADDING A TRUNK GROUP AND MEMBERS

This flowchart illustrates the assignment of a trunk group and its associated members. When a new group is defined, assign at least one member even if it is a "dummy." Trunk members may be changed individually or on a group basis.

NOTE: Caution must be exercised when changing members as a whole group, because certain field values may result in default values being assigned that are undesired.

- Use view 5.3 to define and insert transmission class data, if required.

  NOTE: Switch software will automatically apply 0dB loss on CCC trunks, regardless of the selected transmission class.

- Use view 5.1 to assign a trunk group to the database.
- Use view 5.5 to add member number(s) to the group.
- Execute RST:TRK command to restore CALEA trunks to service. RST:TRK can be used to restore individual trunks, a range of trunk members in a group, or a complete trunk group.

Refer to Figures 3-8 and 3-9 .

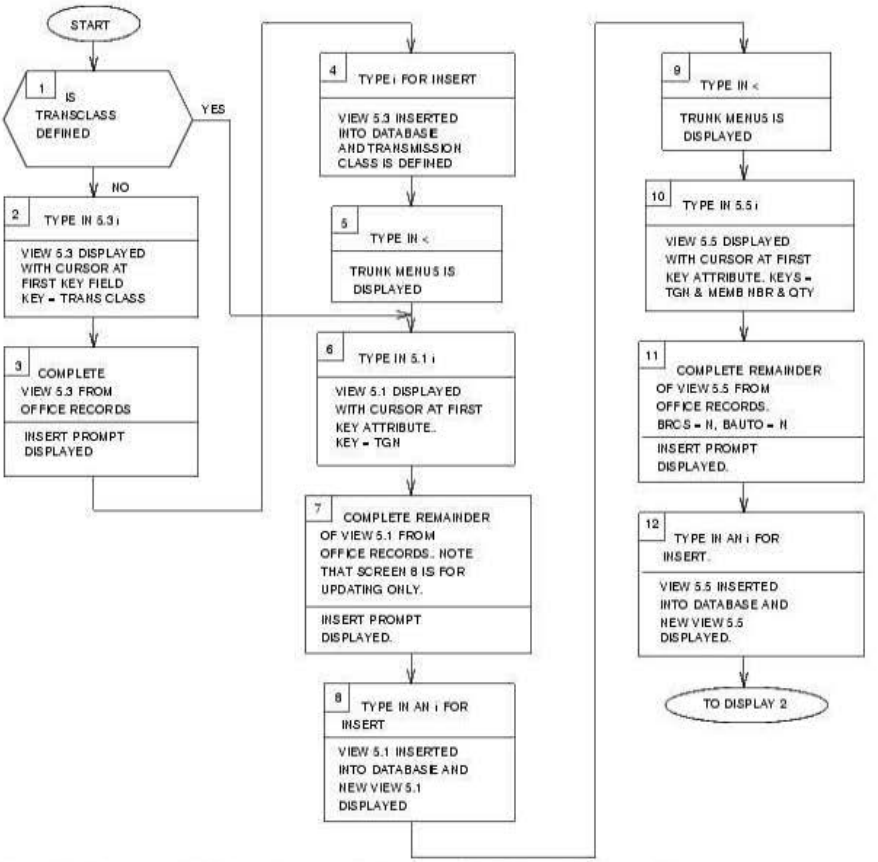


Figure 3-8 Example of Adding a New Trunk Group and Members (Display 1 of 2)

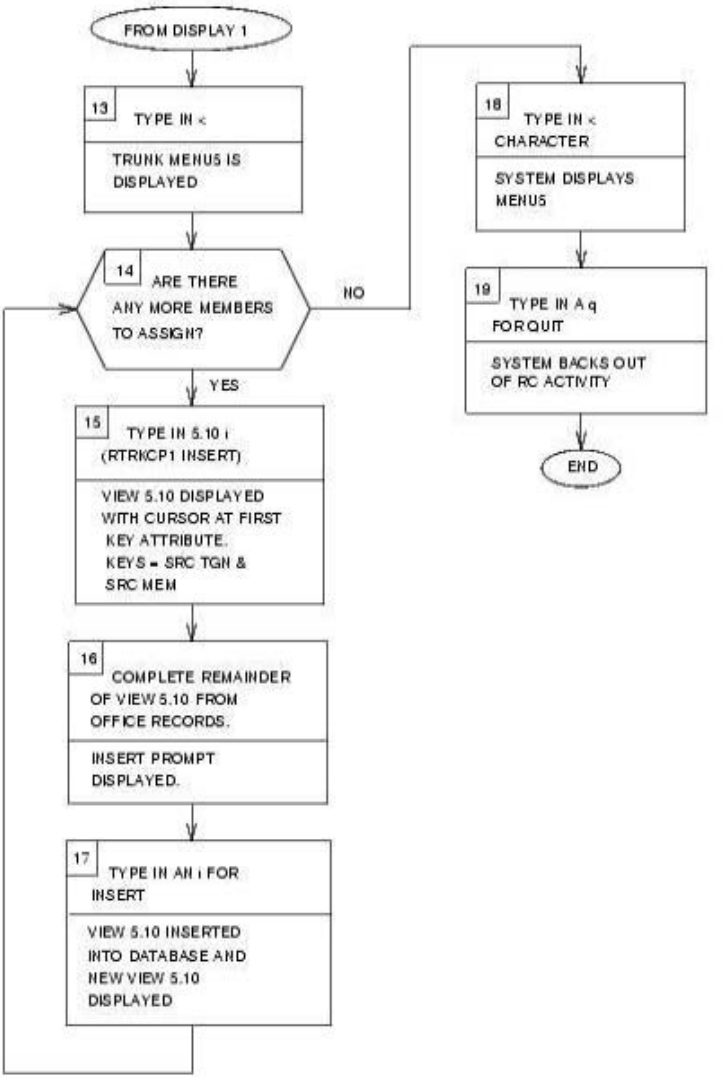


Figure 3-9 Example of Adding a New Trunk Group and Members (Display 2 of 2)

3.9.6.2 DELETING A TRUNK GROUP AND MEMBERS

This flowchart demonstrates the deletion of all members of a trunk group, followed by deletion of the trunk group. View 5.5 is used to delete the members and view 5.1 is used to delete the group.

NOTE: The example assumes the use of "1" for the QTY field on view 5.5. In certain circumstances, this field can be used to delete multiple members with one Recent Change operation.

Refer to Figure 3-10

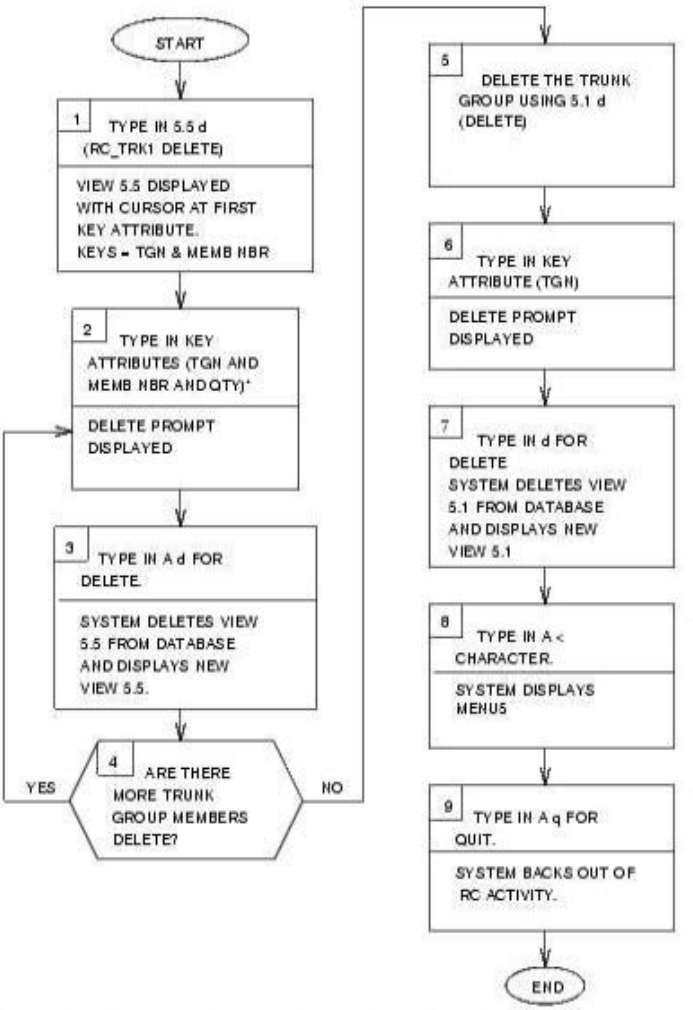


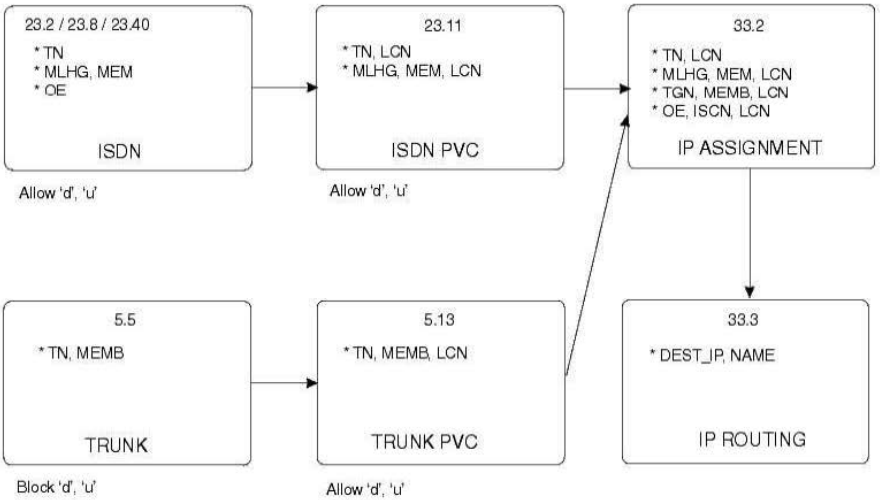
Figure 3-10 Example of Deleting a Member From a Trunk Group Example of Deleting a Member From a Trunk Group

3.10 INTERACTION BETWEEN RECENT CHANGE VIEWS

Figure 3-11 shows the interactions between the new 33.2 and 33.3 Recent Change views and the existing

ISDN and trunk PVC views.

Each of the six "screens" depicted in the flowchart contains several lines of text. The first line lists the applicable view numbers. The lines denoted with an asterisk (*) are the key fields for each of these views. The last line tells whether the view is used for ISDN line or trunk assignments.



Key: 'd' refers to the 'delete' operation via Recent Change
'u' refers to the 'update' operation via Recent Change

Note: updates and deletes are only allowed if the CALEA IN USE bit is not set for underlying data present on RC/V view 33.2

Figure 3-11 Recent Change View Interactions

3.11 CALEA CASE PROVISIONING

Specific surveillance case provisioning is performed by the Surveillance Administrator and is outside the scope of this document.

4. NETWORK TROUBLESHOOTING

4.1 OVERVIEW

A call can fail for many reasons including called party interface busy, destination address is out of order, network busy, etc. When the call fails, the switch will initiate call clearing. Surveillance CDC messages are sent to the SAS terminal to indicate the failures encountered by a monitored call.

If an error condition such as an assert or audit is encountered as a result of this feature set, the normal operation of the subscriber's service will be protected as the first priority.

4.2 UNUSUAL EVENTS HANDLING

Unusual events will be handled by sending reports to the CALEA TTY describing the unusual event and in some cases logging the administrator of the CALEA system if the event was linked to their login session.

4.3 CALL CONTENT CHANNEL (CCC)

4.3.1 CCC TRUNK IS 'OOS'

When a CCC trunk is out of service (OOS), an autonomous report, RMV TRK, is sent to the SAS terminal. The RST:TRK command must be executed from a non-CALEA terminal to put the trunk back in service (IS). A RST TRK report is generated when a CCC is placed back in service.

4.3.2 CCC NOT AVAILABLE

If the switch attempts to access and use a CCC for a given subject and all CCCs provisioned for the surveillance subject are in use, the switch denies allocation of a CCC and the intercepted call content is not transmitted. The switch continues to provide CDC messages (except for CCOpen and CCClose) for the call even if a CCC is not available.

4.3.3 C-TONE FAILURE

Failure to apply the continuity signal to an idle CCC circuit associated with a surveillance is reported using the ContentChannelSetupFailure administration message sent to the Surveillance Administration System. The channel(s) on which the failure occurred and one of the following failure causes are reported:
* Switch blockage - cannot set up CCC for a surveillance
* Resource unavailable - cannot set up CCC for a surveillance
* Other - span failure on the CCC

4.4 CALEA SYSTEM PROCESS (CASP)

4.4.1 OVERVIEW

The CALEA System Process (CASP) is responsible for performing resource allocation for a new surveillance, delivering specific CDC messages to the SAS, and requesting the bridge process (CABR) to perform a bridge action.

A failure detected in or by the CASP will not impact a call in progress.

4.4.2 ERRORS

Requests to the CALEA System Process (CASP) can result in (but are not limited to) the following conditions:

4.4.2.1 Unable to allocate RLcal_info tuple.

If no tuples are available in the idle list, the CASP will not be able to begin a new surveillance for a new call, or extend a surveillance for an existing call ID. This will result in an assert indicating that the limit has been reached in new surveillances or added call legs for existing surveillances. The CASP will report this condition to the surveillance administration ROP.

4.4.2.2 Unable to create a bridge process (CABR).

This condition assumes a CDC channel has already been created for a Level I surveillance. A sanity timer has expired before an acknowledgement has been received from the newly-created CABR. In this case, the required Level II surveillance cannot be established. The surveillance level of the terminal process will be lowered to Level I and a failure report will be sent to the surveillance administration ROP.

4.4.2.3 CABR is unable to create/move a bridge.

This condition should be handled primarily by the CABR, and is noted here only to indicate that the CASP should perform the same recovery actions as the CABR process creation above, that is, the surveillance level of the terminal process will be lowered to Level I and a failure report will be sent to the surveillance administration ROP.

4.4.2.4 ASN.1 encoding failure.

If a message to be sent to the LEA cannot be encoded correctly by ASN.1, an assert will be invoked and the failing message will be discarded.

4.4.2.5 Unknown message received.

The CASP will print out a debug message detailing the "unknown" message and its contents, and then ignore the message and continue with more message reception and processing.

4.4.2.6 Socket-related failure.

Socket-related failures will be handled by the Socket Manager, which will assert and report the failure to surveillance administration ROP. The CASP will not take any further action.

4.5 SOCKETS

4.5.1 OVERVIEW

Sockets is a widely used application program interface to the IP network. A socket is a path that is defined by a pair of addresses; the local internet protocol (IP) address and port number for the transmission control protocol (TCP), and the foreign IP address and port number. Each address/port combination is referred to as a "socket address." Together, both address/port combinations are referred to as a "socket pair" of addresses.

4.5.2 ERRORS

Any socket-related failure will be handled by the Socket Manager by sending a CDC Communications Alarm message to the SAS detailing the failure. The CASP will not assert when a socket failure is encountered.

4.5.2.1 CDC COMMUNICATIONS ALARM MESSAGES

For the CDC alarm messages, see the report:

- REP CALEA SAS ERROR

4.5.2.2 CCC COMMUNICATIONS ALARM MESSAGES

For the CCC alarm messages see the reports:

- RMV TRK
- RST TRK
- REPT CALEA SAS ERROR

4.6 CDC/PDC ERRORS

Problems associated with a surveillance CDC or PDC are reported on the SAS ROP.

NOTE: * = Unexpected, software problems which would cause an assert if encountered.

* The socket is non-blocking and a previous connection attempt has not yet been completed.
+ The connection was refused.
* The domain is not supported.
* Insufficient global memory is available.
* The socket is non-blocking and a connection can not be completed immediately.
* Socklen is not the size of a valid address for the specified address.
*The socket is already connected.
*The socket is of type SO_DGRAM, requiring the data be sent automatically, however the message exceeded internal buffer space.
+ Call establishment error. The TCP/IP platform has received an ICMP_UNREACH message.
* Insufficient global memory to allocate a socket{} structure.
+ The specified socket is not connected.
* The socket does not refer to a valid socket structure.
* The application has requested to send out of band data, however the protocol does not support this functionality.
* The operation requested is not supported for this socket.
* The protocol type or the specified protocol is not supported within this domain.
* Insufficient user memory is available for the socket send queue.
* The socket is marked as non-blocking and the call would block.

These alarm messages will be generated with a "handling priority" equivalent to major alarm but without the audible alarms.

4.7 PH

4.7.1 OVERVIEW

The packet handler (PH) contains the TCP/IP software that routes the PDC subject content to the LEA.

4.7.2 ERRORS

Protocol Monitoring (PM) can be triggered by the following:

- The IP datagram length,
- the IP version,
- checksum error,
- illegal IP source address,
- illegal IP destination address,
- invalid IP header,
- invalid protocol field (not supported),
- no outgoing route available,
- invalid IP option was received, or
- the source IP address (from the received IP datagram perspective).

NOTE: The local IP address mentioned above is actually the destination IP address in received datagrams and the source IP address in IP datagrams that are sent out. If only the local IP address is specified, then the first IP datagram with the local address is received will fire the trigger. As just stated, the default trigger is the local IP address which is a required parameter.

4.8 CALEA PACKET ERRORS

When packet errors occur in the CMP, SMP, or PH, the **REPT CALEA SAS** report is sent to the surveillance terminal. The report contains information regarding

- the processor environment where the error message originated (PSUPH or SM)
- the event number
- the time of day
- the description of the error type

  ERROR 14 = Protocol Handler Resource CAL_INFO Exhaustion

  ERROR 15 = Invalid Protocol Handler CAL_INFO attribute value

  ERROR 17 = RLCASE_IDX data inconsistency

  ERROR 18 = RLCASE_IDX tuple missing

ERROR 19 = RLLAESCASE tuple missing

ERROR 22 = Attempted to add monitoring station when 5 already exist

ERROR 23 = Attempt to send a CALEA message to a CALEA process failed

ERROR 24 = PSLAESCASE tuple missing when adding new monitoring station

- a description of the data type associated with the error type
- and, the data value(s) in hexadecimal format associated with a specific data type

For the complete report description, see Chapter 6 .

4.9 TONE DECODER OVERLOAD (5E15 and later)

Excessive UTD usage can block originations from lines and multi-frequency (MF) trunks. This may cause an unacceptable level of dial tone delay or failed calls. Corrective actions may include:

- Growing additional UTD circuits. Refer to 235-105-231, *Hardware Change - Growth*, for the procedures.
- Re-designating some subjects from DTMF STATUS=ESSENTIAL to DTMF STATUS=STANDARD on view C.4. This is view can only be accessed by the Surveillance Administrator.
- Reducing the value of "TD LIMIT" on RC/V view 8.1. Note that the value of "TD LIMIT" on view 8.1 has no effect on cases marked DTMF STATUS=ESSENTIAL on view C.4.
- Re-assign subjects to SMs with a lighter UTD usage (where physically possible).

4.10 TONE DECODER ALARM MESSAGE (5E15 and later)

The switch sends a REPT CALEA SAS report to the SAS terminal whenever a tone decoder is dropped from a surveillance or cannot be attached to a surveillance.

The alarm message contains the caseID and one or more of the following error type messages:

- **Tone Decoder Dropped Due to Load**

  CALEA tone decoder threshold was exceeded. See Section 3.7 for procedures covering tone decoder threshold modification.

- **Digit Surge Tone Decoder Dropped**

  A burst of digits greater than 100 digits in 20 seconds occurred. No action required.

- **Tone Decoder Dropped**

  Tone decoder dropped due to other failure/maintenance.

- **No Tone Decoder Available**

Additional tone decoders may need to be provisioned in the office.

The alarm report is generated with a handling priority equivalent to 'PHMNORM" (a normal priority message requiring some action to be taken by switch personnel).

For the complete report description, see Chapter 6 .

4.11 AUDITS

4.11.1 OVERVIEW

Audits are responsible for detecting lost resources and data structure inconsistencies. If an error is detected, audits take actions (either directly or indirectly) to recover the lost resources and correct inconsistencies before they adversely affect the system. The following is an overview of the audit changes in the SM and the PH that ensure the integrity of data added and modified.

4.11.2 NEW AND MODIFIED AUDITS

The following is an overview of the audit changes in the SM that ensure the integrity of data added and modified by this feature set.

- BRGDB

  The BRGDB audit ensures the integrity of the RLBRGDB relation.

- CALINFO

  The CALINFO audit ensures the integrity of the new RLCAL_INFO relation.

- CCBCOM and CHDB

  The CCBCOM and CHDB audits are modified to recognize the new linkage from the RLCCBCOM relation to the RLBRGDB relation.

- CRECORD

  The CRECORD audit is modified to recognize the new linkage from the RLCRECORD relation to the new RLCAL_INFO relation.

- PORTLA

  The PORTLA audit is modified to ensure the integrity of the new attributes added to the RLPORTLA relation by this feature.

The following is an overview of the audit changes in the PH that ensure the integrity of data added and modified by this feature set.

- LAESCASE

  The LAESCASE audit ensures the integrity of the new PSlaescase[\0] array and its associated headcell (PSrlaescasehd).

- CALINFO

  The CALINFO audit ensures the integrity of the new PScal_info[\0] array and its associated headcell (PSrcal_infohd).

- ALDB

  The ALDB audit has been modified to ensure the integrity of the new semantic linkage between the PSaldb[\0] array and the PSlaescase[\0] array.

- LCCB

  The LCCB audit has been modified to ensure the integrity of the new semantic linkage between the PSllcb[\0] array and the PScal_info[\0] array.

4.11.3 KEEP ALIVE AUDITING

There are several scenarios in which the CALEA bridge process (CABR) can become stuck in a busy state. It may be that the CABR terminal process did not receive a mgIDLE_PT message, the corresponding originating terminal process (OTP) or terminating terminal process (TTP) is purged, SM selective or full initialization has occurred, or due to audit recovery. Therefore, keep alive auditing is performed between the CABR terminal process and the CALEA system process (CASP).

The TCP socket application turns on the keep-alive mechanism by setting the keep-alive timer to 5 minutes to detect the failure cases. Once a failure case is detected, a error handling function (provided by the application) is invoked by the TCP/IP platform to perform the error handling.

4.12 OVERLOAD CONTROL (OC)

4.12.1 SRE RESOURCES

Overload Control (OC) is the SRE resource exhaustion reporting mechanism. All SRE resources under OC have at least one idle list which is managed by the application using specialized Dynamic Access (DA) primitives created explicitly for the dynamic relation. When a monitored resource exhausts due to no more idle resources available, DA calls Integrity Monitor (IM). IM schedules a immediate audit to attempt to recover any resources that may have been idled incorrectly, left dangling, etc. IM sets a bit in the OCrscmon[] table for the resource. This tells OC to start monitoring this resource every six-seconds until the overload has cleared. The audit probably will not recover any resources. The resource will be in overload for a minimum of 18 seconds. If this is the first overload in the particular SM during the current 15 minute interval, an OP OVRLD message will be output to the ROP.

4.12.1.1 CALINF RESOURCE EXHAUSTION

In the case of CALINF resource exhaustion, OP OVRLD reports will appear on the MCC TTY, for example:

```
*  OP OVRLD SM=2
     REAL TIME NONE
     RESOURCE  CALINF
     CONTROLS  DNET
     CONTROLS  AVRT
```


NOTE: The control AVRT (Avoidance Routing) applies to calls involving one-way trunks and is administered by RTA. DNET (Defer Non-Essential Task) is a "maintenance" control looked at by only a very few maintenance tasks (REX, certain diagnostics, etc.) These controls, by design, do not block calls but attempt to route around the problem, but will NOT fail a call specifically due to the overload.

In addition, REPT CALEA SAS reports will appear on the Surveillance Administration System TTY, for example:

```
   REPT CALEA SAS ERROR SM=2  EVENT=37 TIME=21:07:20
     ERROR TYPE=Surveillance not started due to SM RLCAL_INFO Exhaustion
     DATA1 TYPE=RLCASE_IDX Relation Key Value
     00060000
     DATA2 TYPE=NONE
     DATA3 TYPE=NONE
     DATA4 TYPE=NONE
```

4.12.1.2 BRGDB RESOURCE EXHAUSTION

In the case of BRGDB resource exhaustion, OP OVRLD reports will appear on the MCC TTY, for example:

```
*  OP OVRLD SM=2
     REAL TIME NONE
     RESOURCE  BRGDB
     CONTROLS  DNET
     CONTROLS  AVRT
```

and craft asserts print on the MCC TTY, such as:

```
A  REPT MANUAL ACTION ASSERT=23063 SM=2  EVENT=3
     PCallocbrg.c AT LINE 65
     Bridging Data Blocks Exhausted
```

In addition, REPT CALEA SAS reports will appear on the Surveillance Administration System TTY, for example:

```
   REPT CALEA SAS ERROR SM=2  EVENT=37 TIME=21:07:20
     ERROR TYPE=Bridge Resource Failure
     DATA1 TYPE=SM Process Identification value
     00060000
     DATA2 TYPE=NONE
     DATA3 TYPE=NONE
     DATA4 TYPE=NONE
```

4.12.1.3 RESOURCE EXHAUSTION RECOVERY

When a CALINF or BRGDB resource exhaustion occurs, Recent Change view 8.40, SRE INCREMENTAL GLOBAL PARAMETERS, must be updated via the normal Recent Change terminal (not the SAS) to increase the number of resources on the switching module listed in the reports.

```
                                    5ESS SWITCH
                                  RECENT CHANGE  8.40
(5547)                  SRE INCREMENTAL GLOBAL PARAMETERS

*1. MODULE              ___
```



```
*2. SOFTWARE RESOURCE    _______
#3. TUPLES TO ADD        ___

    INCREMENTAL VALUE    _____
    CURRENT TOTAL VALUE  _____

    WARNING: This form should not be used to make changes to
             dynamic memory without first contacting your
             next level of support. Refer to the Administration
             Guideline Section for Software Resource Engineering.
```

For CALINF, set:
MODULE = switching module that ran out of resources.
SOFTWARE RESOURCE = CAL_INF
TUPLES TO ADD = the number of tuples by which you want this resource increased or decreased (-50 to 50). The default number of total resources is 25.

For BRGDB, set:
MODULE = switching module that ran out of resources.
SOFTWARE RESOURCE = BRGDB
TUPLES TO ADD = the number of tuples by which you want this resource increased or decreased (-50 to 50). The default number of total resources is 64.

If the resource is not increased, subsequent surveillances will not occur.

4.12.2 PH RESOURCES

An overload condition occurs due to too many surveillances on a subject PH or too much traffic on a delivery PH. PH resource exhaustion is reported as always, via OP OVRLD reports to the MCC TTY. Refer to 235-600-750, *5ESS® Switch Output Messages*, for an explanation of the output message(s) and the appropriate action(s) to be taken.

5. MAINTENANCE

5.1 OVERVIEW

The CALEA feature set will block routine maintenance activities (100-108 and digital loopback) for CCCs.

When either a resource is not restored properly or the far end equipment is not restored, leaving the resource out of service preventing its use in delivering content, the SAS will be notified of any out of service condition on a CCC, CDC or PDC.

5.2 PORT STATUS ADMINISTRATION (PSA)

PSA is responsible for maintaining and reporting the status of ports on the switch. The RMV TRK report is sent to the SAS whenever a CCC trunk is placed out of service (OOS). This output message will generate an alarm with a "handling priority" equivalent to a major alarm but with out the audible alarms.

An autonomous report, sent to the SAS, will also be generated when a CCC is placed back in-Service (IS) using the same "handling priority" and message class.

5.3 ODBE ACCESS TO CALEA DATA

For the purposes of troubleshooting and maintenance, ODBE will have update access to all data except the global parameter GLCALIPADR. GLCALIPADR is viewable, but has been blocked from ODBE update. Any attempt to change GLCALIPADR via ODBE will result in the response: **You are not allowed to update this office parameter using ODBE**.

5.4 SM INITIALIZATIONS (FULL/SELECTIVE)

If a monitored call is dropped by an initialization, there is no notification to the LEA, and there is no attempt to re-establish surveillance on the current call. The surveillance will be established starting with the subject's next call. All the surveillance-related information shall be preserved. All the SM dynamic data will be reset during a full SM initialization. Full initializations with or without pump will reestablish the PDC socket connections.

In 5E15 and later software releases, tone decoders are dropped from post cut-through surveillance calls during a selective initialization on an SM.

For Level I subjects, if the tone decoder is dropped, a message announcing the drop is sent to the SAS terminal and the LEA collection facility, but CDC communication continues as normal. For Level II subjects, if the tone decoder is dropped, a message announcing the drop is sent to the SAS terminal and the LEA collection facility, however, CCC and CDC communication continue as normal.

5.5 AM INITIALIZATIONS

During a manual and automatic full AM initialization up through and including D4 level (init 54), all surveillance static data is preserved. An active call and the surveillance are dropped, but the surveillance is established again when the subject initiates a new call. All the AM dynamic data will be reset during a full AM initialization and need to be re-initialized.

5.6 PH INITIALIZATIONS

During PH selective initialization (soft switch), CDC/PDC connections are preserved and any queued data for both transmit and receive remains unaffected.

A PH full initialization (hard switch), results in PDC socket connections being re-established after initialization.

5.7 TRUNK OOS/IS

The switch will send an alarm message to the SAS whenever a CALEA trunk is taken out of service and restored to service. This report will be the same as the existing RMV TRK output message that reports trunk port status. There is no audible alarm.

5.8 SOFTWARE RELEASE RETROFIT AND LARGE TERMINAL GROWTH

During a software release retrofit, the monitored calls will not be impacted by the CALEA feature. The monitoring connections (CCC and CDC channels) will be dropped. Since all the existing dynamic data for the stable calls is reset, the monitored calls are not considered as monitored calls anymore during and after retrofit.

5.9 TRUNK & LINE WORK STATION (TLWS)

5.9.1 TREATMENT FOR CCC TRUNKS

TLWS will block all tests on CCC trunks.

5.9.2 TREATMENT OF SUBSCRIBER LINES UNDER SURVEILLANCE

With one exception, TLWS test calls will not have a CALEA surveillance occurring. Since tests do not create a call record, CALEA will not monitor these lines. The one exception is monitor busy idle.

When the talk and monitor phone (also called callback) is added, the callback (CBAK) process is created and associated with the port under test (PUT). The T&M can be added several ways. The various ways the T&M phone can be accessed are:

- The most straight forward case has the T&M phone added as part of process of testing the line either directly by the command requesting it or indirectly as an automatic operation of another test. Once the T&M phone is added, the T&M could be put in the following modes:

  — Talk (equivalent to double bridge)

  — Monitor (equivalent to single bridge)

  — Hold (equivalent to single bridge)

  Simply adding the T&M to a subject's line via these methods (pokes 4301, 4302, 4303 or 4304), would not cause LEA monitoring to occur since the subject does not go offhook, but the potential for activating the surveillance bridge is there especially since the TLWS can ring the line.

- 101TL calls.

  The 101TL call begins when the 101TL DN is dialed from the subject's line. The 101TL call is initially processed in POTS call processing. TMlotck() is called to start the terminal maintenance portion of the

101TL setup. Since the subject's line is placing a call, LEA monitoring will occur.

- Monitor Busy (poke 4600) and Monitor Busy Idle (poke 4601)

  If the TLWS attempts to seize a line that is busy, the message "DO MNTR BUSY(4600) OR B&I(4601) ONLY" will be displayed. The craft person can then do 4600/4601 (specific actions found starting in TMtmon.c) to add the T&M.

  When the line is idle and the 4601 poke is done, the port is released for the subscriber to use. Any calls to or from that line activates the CBAK process. Monitor Busy Idle does not interfere with the customer's ability to make and receive calls. This means that LEA monitoring can occur during the time monitor busy idle is active.

NOTE: The above cases can be done with either local or remote callback. The remote T&M case goes through call processing code (RTrtereq) as part of the creation of the CBAK process.

5.10 CDC/PDC TRUNK TESTS

Routine or scheduled trunk tests for CDCs and PDCs are handled in the same way as regular packet trunk channel tests. Note that RMV/RST TRK reports are sent to the SAS ROP.

6. INPUT AND OUTPUT MESSAGES

6.1 INPUT COMMAND AND OUTPUT REPORT DESCRIPTIONS

This chapter contains a full description of each input command (also known as an input message) and output report (also known as an output message) referenced within this document. The commands and reports are listed in alphabetical order.

NOTE: These CALEA-specific commands and reports are documented in this information product only. They are not documented in 235-600-700, *Input Messages*.

Input messages are used to control, maintain, and monitor the switching system, including the processors, peripherals, and other software. Output reports are generated either in response to input messages, or to inform support personnel of system conditions or automatic operations that have been performed by the system.

A brief overview of the manual page layout follows. For more information on commands and their usage, refer to 235-600-700, *Input Messages*. For more information on reports and their usage, refer to 235-600-750, *Output Messages*.

6.1.1 INPUT COMMAND DESCRIPTIONS

For the purposes of security and surveillance administration, the following sections of each input command description are of the most value:

The "PURPOSE" section of the manual page contains a brief explanation of the purpose of the message and includes the explanation of any associated warnings.

The "FORMAT" section contains the command format including all options. Parameter values are represented by lowercase letters which are defined in the "EXPLANATION OF MESSAGE" section. Optional parameters are surrounded by brackets '[]'. An OR bar '|' separates a selection of entries enclosed by brackets. Only one of the entries separated by OR bars may be selected.

NOTE: Brackets and OR bars are never used when entering a command. They are only used in message formats to show you how a message must be constructed.

The "EXPLANATION OF MESSAGE" section explains the meaning of the various parameter names, parameter values, and variables in the format. Parameter values are represented by lowercase letters in the command format.

The "SYSTEM RESPONSE" section defines acknowledgments that appears one space after the terminating character of the command. This will normally happen about five seconds after the command is entered.

The "REFERENCES" section contains a list of all related input and output messages.

6.1.2 OUTPUT MESSAGE DESCRIPTIONS

For the purposes of security and surveillance administration, the following sections of each output message description are of the most value:

The "FORMAT" section contains the layout of each output report.

The "REASON FOR OUTPUT" section contains a brief summary of why the message appeared.

The "VARIABLE FIELD DEFINITIONS" section contains the meaning of the various keywords, arguments, and variables shown in the format.

The "ACTION TO BE TAKEN" section contains a brief summary of any actions that should be taken in response to the output message.

The "ALARMS" section contains any alarms that are associated with the output message.

The "REFERENCES" section contains all related input and output messages.

6.2 ASGN:SECRTY command

```
                                        ID.............ASGN:SECRTY
                                        RELEASE........5E14 and later
                                        COMMAND GROUP..AUTH
                                        APPLICATION....5
                                        TYPE...........Input


1.  PURPOSE

    This command will be used by the switch System Administrator to
    assign a default user ID and password to be used by the
    Surveillance Administration System (SAS) Security Administrator.
    The switch System Administrator will have to execute this command
    from a non-SAS terminal.


2.  FORMAT

    ASGN:SECRTY,USRID="a";


3.  EXPLANATION OF MESSAGE

    a       = The user ID (3 to 8 characters in length).


4.  SYSTEM RESPONSE

    PF      = Printout follows.


5.  REFERENCES

    Output Message(s):
      ASGN SECRTY
```

6.3 ASGN SECRTY report

```
                                        ID.............ASGN:SECRTY
```

```
                                        RELEASE........5E14 and later
                                        MESSAGE CLASS..NOCLASS
                                        APPLICATION....5
                                        TYPE...........Output
```

1. FORMAT

```
ASGN SECRTY
a
```

2. REASON FOR OUTPUT

To report the result of assigning a Security Administrator user ID and password to the Surveillance Administration System.

3. VARIABLE FIELD DEFINITIONS

a = Status of the command:

```
     COMMAND COMPLETED SUCCESSFULLY
     FAILED, TUPLE COUNT EXCEEDED
     USER ID MUST BE 3-8 CHARACTERS
     PASSWORD MUST BE 6-12 CHARACTERS
     A SYSTEM ERROR OCCURRED TRY AGAIN
     THE USER ID ENTERED ALREADY EXISTS
```

4. ACTION TO BE TAKEN

If "COMMAND COMPLETED SUCCESSFULLY", no action needs to be taken.
If "FAILED, TUPLE COUNT EXCEEDED", the maximum number of users has been exceeded; a user must be deleted to add a new user.
If "USER ID MUST BE 3-8 CHARACTERS", enter a valid user ID.
If "PASSWORD MUST BE 6-12 CHARACTERS", enter a valid password.
If "A SYSTEM ERROR OCCURRED TRY AGAIN", try command again later.
If "THE USER ID ENTERED ALREADY EXISTS" enter a different user ID.

5. ALARMS

None.

6. REFERENCES

Input Message(s):
ASGN:SECRTY

6.4 DEL:SECRTY command

```
                                        ID.............DEL:SECRTY
                                        RELEASE........5E14 and later
                                        COMMAND GROUP..AUTH
                                        APPLICATION....5
                                        TYPE...........Input
```

1. PURPOSE

   This command is used by the switch System Administrator to delete a user ID and password of Surveillance Administration System (SAS) Security Administrator. The switch System Administrator will have to execute this command from a non-SAS terminal.

2. FORMAT

   DEL:SECRTY,USRID="a";

3. EXPLANATION OF MESSAGE

   a = The user ID (from 3 to 8 characters in length).

4. SYSTEM RESPONSE

   PF = Printout follows.

5. REFERENCES

   Output Message(s):
   DEL SECRTY

6.5 DEL SECRTY report

```
                                        ID.............DEL:SECRTY
                                        RELEASE........5E14 and later
                                        MESSAGE CLASS..NOCLASS
                                        APPLICATION....5
                                        TYPE...........Output
```

1. FORMAT

   DEL SECRTY
   a

2. REASON FOR OUTPUT

To report the result of deleting a Security Administrator user ID from the Surveillance Administration System.

3. VARIABLE FIELD DEFINITIONS

a = Status of the command:

COMMAND COMPLETED SUCCESSFULLY
USER ID DOES NOT EXIST
USER ID IS NOT A SECURITY TYPE
A SYSTEM ERROR OCCURRED TRY AGAIN

4. ACTION TO BE TAKEN

If "COMMAND COMPLETED SUCCESSFULLY", no action needs to be taken.
If "USER ID DOES NOT EXIST", check user ID spelling.
If "USER ID IS NOT A SECURITY TYPE", cannot delete a surveillance administrator.
If "A SYSTEM ERROR OCCURRED TRY AGAIN", try again later.

5. ALARMS

None.

6. REFERENCES

Input Message(s):
DEL:SECRTY

6.6 EXC:PING command

MESSAGE NAME...EXC:PING
RELEASE.....5E14 and later
COMMAND GROUP..TRKLN
APPLICATION....5
TYPE.....Input

1. PURPOSE

The Packet Internet Groper (PING) is used to verify a Transmission Control Protocol/Internet Protocol (TCP/IP) connection between the Source Internet Protocol (SRCIP) address and the Internet Protocol Destination (IPDEST) address. PING sends a request message with data to the IPDEST address and expects a reply from IPDEST, returning the data sent in the request.

Note: Only one EXC:PING input message is allowed per SM or CHNG until the EXC:PING processing is complete. The system response will indicate when the EXC:PING is still in progress. The response message is RL - PING IN PROGRESS. To enter a valid EXC:PING, repeat the input message after a EXC:PING output.

2. FORMAT

[1] EXC:PING,SM=a[,SRCIP=e.f.g.h][,BYTES=i]...
...[,TIMEOUT=j][,REPEAT=k],IPDEST=l.m.n.o;

[2] EXC:PING,CHNG=a-b-c-d[,SRCIP=e.f.g.h][,BYTES=i]...
...[,TIMEOUT=j][,REPEAT=k],IPDEST=l.m.n.o;

3. EXPLANATION OF MESSAGE

a = SM number.

b = PSU unit number. Refer to the APP:RANGES appendix in the Appendixes section of the Input Messages manual.

c = PSU shelf number. Refer to the APP:RANGES appendix in the Appendixes section of the Input Messages manual.

d = Channel group (CHNG) number. Refer to the APP:RANGES appendix in the Appendixes section of the Input Messages manual.

Note: Source IP (SRCIP) is the address the PING is sent from. Each entry (e-i) is part of the SRCIP address. The default is the SRCIP of the SM or CHNG.

e = SRCIP. This is the address the PING is sent from. The range is 0-255.

f = SRCIP. The range is 0-255.

g = SRCIP. The range is 0-255.

h = SRCIP. The range is 0-255.

i = BYTES to send in PING Message. This is the number of bytes that will be sent to the IPDEST and the same number of bytes received from the IPDEST. The range is 1-126. The default is 126.

j = TIMEOUT in seconds waiting from a reply from IPDEST. The range is 1-10. The default is 5.

k = REPEAT the number of times to send the message to IPDEST.

The range is 1-5. The default is 3.

Note: IP Destination (IPDEST) is the address the PING is sent to. Each entry (l-o) is part of the IPDEST address.

l = IPDEST. The range is 0-255.

m = IPDEST. The range is 0-255.

n = IPDEST. The range is 0-255.

o = IPDEST. The range is 0-255.

4. SYSTEM RESPONSE

NG = No good. The message was not accepted because the SM is isolated or the equipment does not exist.

NG - NOT VALID FOR PH = No Good. The EXC:PING is not valid for this PH. The feature is not equipped on this PH.

NG - NOT VALID FOR SM = No Good. The EXC:PING is not valid for this SM. The feature is not equipped for this SM.

NG - NOT VALID PROCESSOR = No Good. An invalid processor type was requested, other than SM or PH.

PF = Printout follows. The message was accepted and a printout will follow.

RL - PING IN PROGRESS = Retry Later - Only one ping input message is allowed to execute on the same SM or PH.

RL - CREATE PING TP FAILED = Retry Later - Failed to create the PING Terminal Process.

RL - MESSAGE TO PING TP FAILED = Retry Later - Message sent to the PING Terminal Process Failed.

RL - TIMEOUT WAITING TO PROCESS PINGDATA = Retry Later - A timeout occurred waiting for the PING DATA message in the PING Terminal Process.

RL - BAD DEFAULT = Retry Later - An incorrect message was received in the PING Terminal Process.

RL - SOCKET NOT CREATED = Retry Later - A socket could not be created.

RL - BIND FAILED = Retry Later - A BIND to the socket could not be completed.


```
    RL - SOCKOPT FAILED(BLKING) = Retry Later - When setting BLOCKING
             for this application, a failure occurred.

    RL - SOCKOPT FAILED(TO) = Retry Later - When setting the TIMEOUT
             for this application, a failure occurred.


5. REFERENCES

     Output Message(s):
       EXC:PING

     Other Manual(s):
       235-105-110 System Maintenance Requirements and Tools
```

6.7 EXC PING report

```
                                                MESSAGE NAME...EXC PING
                                                RELEASE........5E14 and later
                                                MESSAGE CLASS..TRKLN
                                                APPLICATION....5
                                                TYPE...........Output


1.  FORMAT

    [1]  EXC PING REPLY FROM SM=a

    [2]  EXC PING REPLY FROM CHNG=a-b-c-d
         PH IMAGE TYPE = e
         SOURCE IP = f
         DESTINATION IP = g
         BYTES SENT = h
         TIMEOUT = i

         PING TIME    STATUS
         j    k       l
         .    .       .
         .    .       .
         .    .       .

 2.  REASON FOR OUTPUT

     To output PING information that is sent from an SM or PH.

     Format 1 is printed in response to an EXC:PING input message
     where an SM is INPUT.  Format 2 is printed in response to an
     EXC:PING input message where a CHNG is INPUT.


 3.  VARIABLE FIELD DEFINITIONS
```

```
a       = SM number.

b       = PSU unit number.

c       = PSU shelf number.

d       = Channel group (CHNG) number.

e       = The image type of the PH. If not a PH, this field
          will read NULL IMAGE.

f       = Source IP address. If zero is displayed the default
          source address is used.

g       = Destination IP Address.

h       = Bytes sent.

i       = The timeout value, in seconds.

j       = The number of PINGs sent.

k       = The time it takes to receive the PING, in milliseconds.

l       = Status of the PING request.


4.  ACTION TO BE TAKEN

    None


5.  ALARMS

    None.


6.  REFERENCES

    Input Messages
      EXC:PING
```

6.8 OP:TCPIP:RTDMP command

```
MESSAGE NAME...OP TCPIP RTDMP
RELEASE........5E14 and later
COMMAND GROUP..TRKLN
APPLICATION....5
TYPE...........Input
```

```
1.  PURPOSE

    The TCP/IP route dump input message is used to verify TCP/IP routing
    tables in an SM or PH.


2.  FORMAT

    [1]     OP:TCPIP:RTDMP,SM=a;

    [2]     OP:TCPIP:RTDMP,CHNG=a-b-c-d;


3.  EXPLANATION OF MESSAGE

    a       = SM number.

    b       = PSU unit number.

    c       = PSU shelf number

    d       = Channel group (CHNG) number.

4.  SYSTEM RESPONSE

    NG      = No good.  The message was not accepted because the SM
              is isolated or the equipment does not exist.

    NG - NO ROUTE TABLES ENTRIES FOUND = No Good.  No entries were
              found in the ROUTE TABLE on the SM or PH requested.

    PF      = Printout follows.  The message was accepted and a
              printout will follow.


5. REFERENCES

   Output Message(s):
     OP TCPIP RTDMP

   Other Manual(s):
     System Maintenance Requirements and Tools
```

6.9 OP TCPIP RTDMP report

```
MESSAGE NAME...OP TCPIP RTDMP
RELEASE........5E14 and later
MESSAGE CLASS..TRKLN
APPLICATION....5
TYPE...........Output
```

1. FORMAT

[1] OP TCPIP RTDMP ROUTE TABLE DUMP FOR SM=a PAGE e OF f
PH IMAGE TYPE = g

ROUTE NUMBER	DESTINATION IP ADDR	DESTINATION IP MASK	GATEWAY IP ADDR
h	i	j	k
.	.	.	.
.	.	.	.
.	.	.	.

ROUTE METRIC	INTERFACE NUMBER	NEXT ROUTE PTR	PREVIOUS ROUTE PTR
l	m	n	o
.	.	.	.
.	.	.	.
.	.	.	.

[2] OP TCPIP RTDMP ROUTE TABLE DUMP FOR CHNG=a-b-c-d PAGE e OF f
PH IMAGE TYPE = g

ROUTE NUMBER	DESTINATION IP ADDR	DESTINATION IP MASK	GATEWAY IP ADDR
h	i	j	k
.	.	.	.
.	.	.	.
.	.	.	.

ROUTE METRIC	INTERFACE NUMBER	NEXT ROUTE PTR	PREVIOUS ROUTE PTR
l	m	n	o
.	.	.	.
.	.	.	.
.	.	.	.

2. REASON FOR OUTPUT

To output TCP/IP routing information that is contained on an SM or PH.

Format 1 is printed in response to an OP:TCPIP:RTDMP input message where an SM is INPUT. Format 2 is printed in response to an OP:TCPIP:RTDMP input message where an CHNG is INPUT.

The Route Number pertains to all values in ('h'-'o').

3. VARIABLE FIELD DEFINITIONS

a = SM number.

b = PSU unit number.

c = PSU shelf number.

d = Channel group (CHNG) number.

e = Current page number.

f = Total number of pages for this output.

g = The image type of the PH.
If not a PH this field will read NULL IMAGE.

h = The route number.
The physical position of the route in the route table.

i = Destination IP Address.

j = Destination IP Mask.

k = Gateway IP Address.

l = The route metric.

m = Interface Number for this route.

n = The Next Route Pointer. If this field has an ENTRY other than 0xffffffff, it will point to the next route entry. If the field has 0xffffffff as an entry, there is no Next Route.

o = The previous route pointer. If this field has an ENTRY other than 0xffffffff, it will point to the previous route entry. If the field has 0xffffffff as an entry, there is no Previous Route.

4. ACTIONS TO BE TAKEN

None.

5. ALARMS

None.

6. REFERENCES


```
Input Message(s):
  OP:TCPIP:RTDMP
```

6.10 REPT CALEA SAS report

```
                                        MESSAGE NAME...REPT CALEA SAS
                                        RELEASE........5E14 and later
                                        MESSAGE CLASS..SECLEA
                                        APPLICATION....5
                                        TYPE...........Output
```

1. FORMAT

```
REPT CALEA SAS ERROR a [f] EVENT=h TIME=ii:ii:ii
  ERROR TYPE = et
  DATA1 TYPE = d1
  [j1 j2 j3 j4 j5 j6 j7 j8]
  DATA2 TYPE = d2
  [k1 k2 k3 k4 k5 k6 k7 k8]
  DATA3 TYPE = d3
  [l1 l2 l3 l4 l5 l6 l7 l8]
  DATA4 TYPE = d4
  [m1 m2 m3 m4 m5 m6 m7 m8]
```

2. REASON FOR OUTPUT

To report the occurrence of a TCP/IP connection breakdown. When the CDC or PDC connection is down, or the socket interface is broken, a communication alarm message is sent to the SAS. For a given MS IP address, only one alarm message is sent to the SAS for any failure cases.

3. VARIABLE FIELD DEFINITIONS

a = The processor environment where the error message originated. The environment can either be the Packet Switching Unit Protocol Handler (PSUPH) which is also referred to as the physical PH address, or the Switching Module (SM).

Valid values(s):

PSUPH=b-c-d-e
- b = Switching module (SM) number.
- c = Packet switching unit (PSU) number.
- d = PSU shelf number.
- e = PSUPH number.

SM=b
- b = Switching module (SM) number.

```
f       = The Channel Group (CHNG) assignment if and only if the
          error message originated from the PH whose PSUPH address
          is indicated above.  The CHNG value is also referred to
          as the logical PH address.  If the error message did not
          generate from the PSU, then this field is left blank.

          Valid values(s):

          CHNG=b-c-d-g
            b       = Switching module (SM) number.
            c       = Packet switching unit (PSU) number.
            d       = PSU shelf number.
            g       = Channel Group (CHNG) number.


h       = Event number

i       = Time of the day the message was generated, in the form
          hours:minutes:seconds.

et      = Description of ERROR TYPE message that was sent to the SAS:
          For a more detailed description of the CALEA SAS error
          report, see section 6.15.

          Valid types(s):

     Attempt to send a CALEA message to a CALEA process failed
     Attempted to add monitoring station when 5 already exist
     Bridge Resource Failure
     Bridge Loop Channel Unavailable
     CCC Dial Out Answer Timeout
     CCC Dial Out connection dropped
     CCC Dial Out fanout not supported
     CCC Dial Out RCV path failed
     CCC Dial Out retry failed
     CCC Dial Out three port conference circuit dropped
     CCC Dial Out three port conference circuit unavailable
     CCC Dial Out unsupported supplementary service encountered
     CCC Dial Out XMIT path failed
     CCCTP can not activate port, can not add
     CCCTP can not close network path
     CCCTP can not idle all ports
     CCCTP can not merge ports on different SMs
     CCCTP can not release all ports
     CCCTP could not remove CTONE
     CCCTP couple port failed, can not add
     CCCTP port access failed, can not add
     CCCTP port limit exceeded, can not add
     CCCTP port limit exceeded, can not merge
```

```
CCCTP port move failed, can not merge
CCCTP received MGINTERRUPT on port
CCCTP rcv can not be accessed
CCCTP trunk hunt failed, can not add
CDC Dial Out connection dropped
CDC Dial Out message queue corrupt
CDC Dial Out message queue full
CDC Dial Out setup failed due to invalid data
CDC Dial Out setup failed, will attempt retry
CDC message dropped, GR30 interface send failed
CDC or PDC Message length invalid
Can not create surveillance bridge
Could not apply CTONE
Destination GR30 LEA CDC DN not recognized by digit analysis
Digit Surge Tone Decoder Dropped
Discarding buffered CDC messages due to inactivity
Error return from close application program interface
Error return from connect application program interface
Error return from getsockdesc application program interface
Error return from getsockname application program interface
Error return from select application program interface
Error return from send application program interface
Error return from setsockopt application program interface
Error return from shutdown application program interface
Error return from socket application program interface
Failed to route to GR30 LEA CDC DN
Failed to send GR30 CDC message to link SM
Found socket data inconsistency
GR30 CAGS TP received MGINTERRUPT
GR30 CAGS/CAGR TP cannot be created
GR30 CDC Connection dropped
GR30 CDC message discarded.  Link occupancy above threshold
GR30 Internal Failure
GR30 Length of CDC message too large for OSDS
GR30 msg queue full, oldest message discarded
HEARTBEAT message dropped, GR30 interface send failed
IAP times out waiting for login digits
Invalid IP route
Invalid LOGIN digits received
Invalid Protocol Handler CAL_INFO attribute value
IP datagram fragment received
LOGIN message dropped, GR30 interface send failed
LOGIN Successful
No FSK or UTD resources available for GR30 interface
No IP route
No Tone Decoder Available
PDC collection facility IP address not obtained
PSLAESCASE tuple missing when adding new monitoring station
Protocol Handler Resource CAL_INFO Exhaustion
RLCASE_IDX data inconsistency
RLCASE_IDX tuple missing
```

```
RLEQUIPDSL tuple missing
RLFC_LINE tuple missing
RLGR30INTF tuple missing
RLLAESCASE tuple missing
RLLAESPROF tuple missing
RLOFFICECODE tuple missing
RLPORTLA tuple missing
RLPR_DNTRAN tuple missing
RLRTDNMOD tuple missing
RLRT_DNTRAN tuple missing
Resource Unavailable
Socket not found
Surveillance not started due to SM RLCAL_INFO Exhaustion
Tone Decoder Dropped
Tone Decoder Dropped Due to Load
Too many IP datagrams received
WARNING: GR30 buffered messages will be discarded in 15 minutes


d1     = Description of DATA1 TYPE associated with the ERROR TYPE above:
d2     = Description of DATA2 TYPE associated with the ERROR TYPE above:
d3     = Description of DATA3 TYPE associated with the ERROR TYPE above:
d4     = Description of DATA4 TYPE associated with the ERROR TYPE above:

         Valid types(s):

 DC Dial Out discarded message
 CDC Dial Out message queue pointers
 CDC or PDC Message length
 CDC event
 CDC LEA DN port status value
 CDC SVC setup request result
 CDC SVC setup response result
 CDC SVC setup state result
 CDC SVC state value
 Collection facility IPv4 address value
 Collection facility TCP port value
 Data collected for collection facility
 Destination SM value
 Error return from sockets application program interface
 Failure return value
 Global Trunk Port value
 Highest socket descriptor value
 IP datagram count
 IP interface identifier
 Lawfully authorized electronic surveillance case data
 LEA destination DN
 Local Trunk Port value
 Logical Protocol Handler Number
 Msg or value
```



```
  NONE (see Note at end of list)
  NUMBER OF PORTS value
  Partial IP datagram dump
  Party Identifier
  Peripheral Control failure value
  PH subscriber CALEA information block
  Protocol Handler Channel Number
  Q.931 Cause Value
  Relation ID Value
  Relation Key Value
  RLCASE_IDX Relation Key Value
  RLLAESCASE Relation Key Value
  RLLAESPROF Relation Key Value
  Routing and Termination failure value
  SM Process Identification value
  Socket descriptor list length
  Socket descriptor value
  Source SM value
  Trunk Group value
  Trunk Member value


j1 - j8  = Data value(s) in hexadecimal format associated
           with a specific DATA1 TYPE above.
           Anywhere from 0 to 8 Data Values can appear.

k1 - k8  = Data value(s) in hexadecimal format associated
           with a specific DATA2 TYPE above.
           Anywhere from 0 to 8 Data Values can appear.

l1 - l8  = Data value(s) in hexadecimal format associated
           with a specific DATA3 TYPE above.
           Anywhere from 0 to 8 Data Values can appear.

m1 - m8  = Data value(s) in hexadecimal format associated
           with a specific DATA4 TYPE above.
           Anywhere from 0 to 8 Data Values can appear.

 For each ERROR TYPE there will always be 4 DATA TYPE lines.
 However, for each non-existent DATA TYPE, "NONE" will print
 instead of a valid data type.

 For each existing DATA TYPE there can be anywhere from 0 to 8
 Data Values. For a non-existing Data TYPE there will be no Data Values.

 Each Data Value consists of a 32-bit word of data associated with
 its corresponding DATA TYPE in the previous line.

 Note that one or more DATA TYPE(S) can be associated with one ERROR
 TYPE, and any particular DATA TYPE can be associated with more than
 one ERROR TYPES.
```

Even though each Data Value can be up to 32 bits in length, some data values will be less, and thus their corresponding output value will be LEFT JUSTIFIED. One needs understanding of the DATA TYPE associated with the Data Values to interpret those values correctly. For example, a 16-bit value of h'001A will appear as h'001A0000.

4. ACTION TO BE TAKEN

Consult field expert to determine the cause/solution of the error in question.

5. ALARMS

None.

6. REFERENCES

None.

6.11 UPD:SECRTY command

```
ID.............UPD:SECRTY
RELEASE........5E14 and later
COMMAND GROUP..AUTH
APPLICATION....5
TYPE...........Input
```

1. PURPOSE

This command will be used by the switch System Administrator to update the Security Administrator's password to a new password. The 5ESS System Administrator will have to execute this command from a non-SAS terminal.

2. FORMAT

```
UPD:SECRTY,USRID="a";
```

3. EXPLANATION OF MESSAGE

a = The user ID (from 3 to 8 characters in length).

4. SYSTEM RESPONSE


```
    PF     = Printout follows.


5.  REFERENCES

    Output Message(s):
      UPD SECRTY
```

6.12 UPD SECRTY report

```
                                                ID.............UPD:SECRTY
                                                RELEASE........5E14 and later
                                                MESSAGE CLASS..NOCLASS
                                                APPLICATION....5
                                                TYPE...........Output


1.  FORMAT

    UPD SECRTY
    a


2.  REASON FOR OUTPUT

    To report the result of updating a Security Administrator password.


3.  VARIABLE FIELD DEFINITIONS

    a  = Status of the command:

         COMMAND COMPLETED SUCCESSFULLY
         PASSWORD MUST BE 6-12 CHARACTERS
         USER ID DOES NOT EXIST
         UPDATE FAILED


4.  ACTION TO BE TAKEN

    If "COMMAND COMPLETED SUCCESSFULLY", no action needs to be taken.
    If "PASSWORD MUST BE 6-12 CHARACTERS, select a valid password.
    If "USER ID DOES NOT EXIST", check user ID spelling.
    If "UPDATE FAILED", try again later.


5.  ALARMS

    None.

6.  REFERENCES
```

```
Input Message(s):
  UPD:SECRTY
```

6.13 VFY SECRTY command

```
ID.............VFY:SECRTY
RELEASE........5E14 and later
COMMAND GROUP..AUTH
APPLICATION....5
TYPE...........Input
```

1. PURPOSE

   This command is used by the switch System Administrator to list all the Security Administrators user IDs entered into the Surveillance Administration System (SAS). The switch System Administrator will have to execute this command from a non-SAS terminal.

2. FORMAT

   VFY:SECRTY;

3. EXPLANATION OF MESSAGE

   No variables.

4. SYSTEM RESPONSE

   PF = Printout follows.

5. REFERENCES

   Output Message(s):
   VFY SECRTY

6.14 VFY SECRTY report

```
ID.............VFY:SECRTY
RELEASE........5E14 and later
MESSAGE CLASS..NOCLASS
APPLICATION....5
TYPE...........Output
```

1. FORMAT


```
VFY SECRTY
a

USER ID     TYPE
b           SECURITY ADMINISTRATOR
.           .
.           .
.           .


2.  REASON FOR OUTPUT

    To report the list of Security Administrators user IDs.


3.  VARIABLE FIELD DEFINITIONS

    a  = Status of the command:

         COMMAND COMPLETED SUCCESSFULLY
         THERE ARE NO ADMINISTRATORS ASSIGNED
         A DATA BASE ERROR HAS OCCURRED TRY AGAIN


4.  ACTION TO BE TAKEN

    If "COMMAND COMPLETED SUCCESSFULLY", no action needs to be taken.
    If "THERE ARE NO ADMINISTRATORS ASSIGNED", information only.
    If "A DATA BASE ERROR HAS OCCURRED TRY AGAIN", try command again.


5.  ALARMS

    None.


6.  REFERENCES

    Input Message(s):
      VFY:SECRTY
```

6.15 CALEA SAS ERROR TYPE DEFINITION

6.15.1 Introduction

This document provides more detailed description of the CALEA SAS error report. It should be considered as supplementary information to the CALEA document 235-200-400. The customers are encouraged to contact Lucent Technical Support and Service Personnel to resolve any issue that may occur.

6.15.2 CALEA SAS Error Types

The following error types are sent to CALEA ROP via the CALEA SAS error report when 5ESS experiences any abnormal condition related to CALEA functionality

Error type:	Attempt to send a CALEA message to a CALEA process failed.
Condition:	OSDS cannot send CALEA related message to a target CALEA process.
Sensitive CALEA Data:	Some scenarios will dump Party Identifier (calling or called party number).
Potential Impact:	Missing a CDC message, or an interception.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Attempted to add monitoring station when 5 already exist.
Condition:	More than 5 LEAs are assigned to this packet subject.
Sensitive CALEA Data:	Party identifier (party member number): Either B1, B2, or D channel, and channel number.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Bridge Resource Failure
Condition:	None
Sensitive CALEA Data:	None
Priority :	N/A
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Bridge Loop Channel Unavailable
Condition:	Cannot bridge into the call, as loop channel is not available.
Sensitive CALEA Data:	Subject's port information
Potential Impact:	No call content is available.
Priority :	High
Action to be considered:	It may be required to relocate lines from this SM other SMs.

Error type:	CCC Dial Out Answer Timeout
Condition:	Law enforcement collection facility for CCC Dial Out did not answer call in specified time.
Sensitive CALEA Data:	None
Potential Impact:	Missing CCC data for surveillance.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCC Dial Out connection dropped
Condition:	Call to CCC destination LEA DN was either cleared or could not be established.
Sensitive CALEA Data:	None
Potential Impact:	Call content is no longer provided to law enforcement.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCC Dial Out fanout not supported
Condition:	Subject to subject redirection resulted in an attempt to merge or fanout call content.
Sensitive CALEA Data:	None
Potential Impact:	Call content is not provided or no longer provided to law enforcement for specified subject/surveillance.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCC Dial Out RCV path failed
Condition:	Attempt to establish CCC dial out subject receive connection failed.
Sensitive CALEA Data:	None
Potential Impact:	Subject receive portion of call content is not provided to law enforcement for affected surveillance.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCC Dial Out retry failed
Condition:	Third attempt to establish CCC dial out connection failed.
Sensitive CALEA Data:	None

Potential Impact:	Call content is not provided to law enforcement for affected surveillance.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCC Dial Out three port conference circuit dropped
Condition:	Conference circuit used to combine subject transmit and receive is no longer available.
Sensitive CALEA Data:	None
Potential Impact:	Call content is no longer provided to law enforcement for specified subject/surveillance.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCC Dial Out three port conference circuit unavailable
Condition:	A Conference circuit to combine subject transmit and receive is not available.
Sensitive CALEA Data:	None
Potential Impact:	Call content is provided in separated mode.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCC Dial Out unsupported supplementary service encountered
Condition:	A supplementary service (e.g., MLHG queuing, queued call pickup) at the intra-switch CCC destination LEA DN was encountered.
Sensitive CALEA Data:	None
Potential Impact:	Call content is not provided to law enforcement.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCC Dial Out XMIT path failed
Condition:	Attempt to establish CCC dial out subject transmit connection failed.
Sensitive CALEA Data:	None
Potential Impact:	Subject transmit portion of call content is not provided to law enforcement for affected surveillance.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP cannot activate port, can not add.
Condition:	Cannot activate an outgoing CALEA CCC digital trunk port. In other words, CALEA cannot gain ownership of the trunk circuit and links the peripheral side data structures to the terminal process.
Sensitive CALEA Data:	Subject's port information.
Potential Impact:	No call content is available.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP cannot close network path
Condition:	The call content channel network path cannot be closed
Sensitive CALEA Data:	Subject's port information
Potential Impact:	No call content is available
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP cannot idle all ports.
Condition:	Cannot successfully release the source and restore C-tone on the trunk.
Sensitive CALEA Data:	None
Potential Impact:	No C-tone is restored.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP can not merge ports on different SMs.
Condition:	Two CCC bridges from different SMs are to be merged and is rejected. Bridge merging is required to merge the bridge and CCC resources associated with multiple subjects when one subject disconnects from a call but the call is not released (e.g. call transfer).
Sensitive CALEA Data:	None

Potential Impact:	One of the CCCs will not have call content.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP can not release all ports
Condition:	Cannot de-couple the ports when more than one port is associated with the PCBLA.
Sensitive CALEA Data:	None
Potential Impact:	Trunk ports are not properly released.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP could not remove CTONE.
Condition:	It occurs when the hardware (e.g., DSU/DSU2) supplying the tone is OOS (high runner case) or Glctone (a global parameter) was overwritten with an invalid value.
Sensitive CALEA Data:	None
Potential Impact:	Call content cannot be successfully delivered.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP couple port failed, can not add.
Condition:	Cannot associate a CCC trunk port with the CALEA process.
Sensitive CALEA Data:	None
Potential Impact:	Call content cannot be successfully delivered.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP port access failed, can not add.
Condition:	Cannot find the port information from relation RLGROUP_PORT.
Sensitive CALEA Data:	None
Potential Impact:	Call content cannot be successfully delivered.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel. It is unlikely unless database is corrupted.

Error type:	CCCTP port limit exceeded, can not add.
Condition:	There are more than 50 CCC trunks to be linked to one PCBLA for adding new CCC scenarios.
Sensitive CALEA Data:	None
Potential Impact:	Call content cannot be successfully delivered.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP port limit exceeded, cannot merge.
Condition:	There are more than 50 CCC trunks to be linked to one PCBLA for merging scenarios.
Sensitive CALEA Data:	None
Potential Impact:	Call content cannot be successfully delivered.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP port move failed, can not merge.
Condition:	Cannot move the PORTLA or CCB to the other CALEA process for merging scenarios. When ports are moved/merged, only the data structures are affected. All hardware related connections are unaffected.
Sensitive CALEA Data:	None
Potential Impact:	Call content cannot be successfully delivered.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP received MGINTERRUPT on port.
Condition:	CALEA receives unexpected message MGINTERRUPT for the CCC trunk.
Sensitive CALEA Data:	None
Potential Impact:	The call content channel will be released.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP rcv cannot be accessed.
Condition:	The receiving CCC trunk PCBLA structure and the CALEA process are not properly linked.
Sensitive CALEA Data:	None
Potential Impact:	The call content cannot be properly delivered.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CCCTP trunk hunt failed, can not add.
Condition:	Cannot allocate CCC trunk successfully.
Sensitive CALEA Data:	None
Potential Impact:	The call content cannot be preperly delivered.
Priority :	High
Action to be considered:	Increase number of CCC trunks.

Error type:	CDC Dial Out connection dropped.
Condition:	SVC for CALEA IP Interface was disconnected due to PH hardware problems or X.25 packet network outage.
Sensitive CALEA Data:	None
Potential Impact:	CALEA CDC data will not be delivered for affected CDC SVC Dial Out surveillance case(s) until hardware/network outage is corrected.
Priority :	High
Action to be considered:	Verify PH and X.25 packet network connections.

Error type:	CDC Dial Out message queue corrupt
Condition:	Software problem.
Sensitive CALEA Data:	None
Potential Impact:	Impact: CDC message(s) in CDC Dial Out (SVC) message queue on specified SM are no longer available to law enforcement.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CDC Dial Out message queue full
Condition:	CDC Dial Out message queue overflowed as a result of no active SVC(s) to establish TCP/IP socket.
Sensitive CALEA Data:	CALEA ASN.1 CDC message dumped to CALEA ROP may have subject's DN and other call identifying information.
Potential Impact:	CDC message(s) dumped on CALEA ROP will no longer be available to send to law enforcement.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CDC Dial Out set failed due to invalid data.
Condition:	SVC-related CALEA surveillance provisioning is incorrect. RC view C.4's SVC LOC LEA CDC TN, SVC DEST LEA CDC TN or RC view 33.2 (IP INTERFACE ASSIGNMENT)/23.40 (X.25 (XAT) PACKET SWITCHING CHANNEL ASSIGNMENT) provisioning for SVC LOC LEA CDC TN is incorrect.
Sensitive CALEA Data:	None
Potential Impact:	CALEA CDC data will not be delivered until provisioned data is corrected. If condition is not corrected, CALEA CDC data will not be delivered to law enforcement collection facilities.
Priority :	High
Action to be considered:	Verify data provisioned on above RC views to CALEA customer documentation.

Error type:	CDC Dial Out setup failed, will attempt retry
Condition:	SVC for CALEA IP Interface could not be established due to OOS XAT logical channel, the X.25 SVC could not be established due to network problems or temporary PH resource contention.
Sensitive CALEA Data:	None
Potential Impact:	CALEA CDC data will not be delivered until XAT logical channel is restored to in-service or temporary network problems are corrected.
Priority :	High

Action to be considered:	Restore OOS XAT logical channel, check X.25 packet network.

Error type:	CDC message dropped, GR30 interface send failed
Condition:	Third attempt to send a CDC message over a GR30 connection failed.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	CDC or PDC Message length invalid
Condition:	The message to be sent to LEA is more than 500 bytes.
Sensitive CALEA Data:	None
Potential Impact:	The call data cannot be properly delivered.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel. It should not happen.

Error type:	Can not create surveillance bridge
Condition:	CALEA bridge process cannot be successfully created to perform interception.
Sensitive CALEA Data:	None
Potential Impact:	The subject call cannot be properly intercepted.
Priority :	Low
Action to be considered:	It should not happen unless the SM is overloaded.

Error type:	Could not apply CTONE
Condition:	CALEA cannot provide CTONE to CCC trunks.
Sensitive CALEA Data:	None
Potential Impact:	No CCC trunks are available if call is intercepted.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Destination GR30 LEA CDC DN not recognized by digit analysis
Condition:	GR30 destination LEA DN doesn't pass digit analysis or has an invalid destination type.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	High
Action to be considered:	Verify the GR30 destination LEA DN.

Error type:	Digit Surge Tone Decoder Dropped
Condition:	A burst of digits greater than 100 digits in 20 seconds occurred.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC dialed digit extraction message.
Priority :	Low
Action to be considered:	Nothing we can do about it.

Error type:	Discarding buffered CDC messages due to inactivity
Condition:	Failed to establish the GR30 CDC Dial out connection in specified time.
Sensitive CALEA Data:	None
Potential Impact:	Queued CDC messages will be dumped to the CALEA ROP.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Error return from close application program interface.
Condition:	Socket cannot be successfully deleted.
Sensitive CALEA Data:	None
Potential Impact:	None. The CALEA socket was closed due no surveillance case using the socket (destination IP address and port). Another CALEA TCP/IP socket will be established if another CDC message needs to be sent.
Priority :	Low
Action to be considered:	None

Error type:	Error return from connect application program interface.
Condition:	Cannot initiate socket connection.
Sensitive CALEA Data:	None

Potential Impact:	CDC cannot be properly delivered.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Error return from getsockdesc application program interface.
Condition:	Cannot retrieve a socket descriptor associated with the local IP address.
Sensitive CALEA Data:	None
Potential Impact:	CDC cannot be properly delivered.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Error return from getsockname application program interface.
Condition:	None
Sensitive CALEA Data:	None
Potential Impact:	None
Priority :	N/A

Error type:	Error return from select application program interface.
Condition:	None
Sensitive CALEA Data:	None
Priority :	N/A

Error type:	Error return form send application program interface.
Condition:	The TCP packet cannot be successfully sent.
Sensitive CALEA Data:	None
Potential Impact:	CDC message cannot be properly delivered.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Error return from setsockopt application program interface.
Condition:	Cannot set socket option.
Sensitive CALEA Data:	None
Potential Impact:	CDC message cannot be properly delivered.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Error return from shutdown application program interface.
Condition:	Cannot shut down the receiving direction for the socket.
Sensitive CALEA Data:	None
Potential Impact:	None
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Error return from socket application program interface.
Condition:	Cannot create a new socket to the destination socket address.
Sensitive CALEA Data:	None
Potential Impact:	CDC message cannot be properly delivered.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Failed to route to GR30 LEA CDC DN
Condition:	Attempt to establish GR30 CDC dial out connection failed.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	High
Action to be considered:	Verify the routing for GR30 destination LEA DN.

Error type:	Failed to send GR30 CDC message to link SM
Condition:	Attempt to send a CDC message to the SM with the GR30 connection failed.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Found socket data inconsistency.
Condition:	Internal socket data structure is corrupted.
Sensitive CALEA Data:	None
Potential Impact:	CDC message cannot be properly delivered.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	GR30 CAGS TP received MGINTERRUPT
Condition:	GR30 process received an unexpected MGINTERRUPT.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	GR30 CAGS/CAGR TP cannot be created
Condition:	GR30 process cannot be created.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	GR30 CDC connection dropped
Condition:	Call to GR30 CDC destination LEA DN was either cleared or could not be established.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	GR30 CDC message discarded. Link occupancy above threshold
Condition:	Attempt to send a CDC message to another SM and the SM to SM link occupancy above threshold.
Sensitive CALEA Data:	None
Potential Impact:	The CDC message will be dumped to the CALEA ROP.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	GR30 Internal Failure
Condition:	Internal failure encountered while processing a CDC message.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	GR30 Length of CDC message too large for OSDS
Condition:	Received a CDC message too large to process.
Sensitive CALEA Data:	None
Potential Impact:	CDC message will be dumped to the CALEA ROP.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	GR30 msg queue full, oldest message discarded
Condition:	The GR30 CDC message buffer is already full when another CDC message is received.
Sensitive CALEA Data:	None
Potential Impact:	The CDC message will be dumped to the CALEA ROP.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	HEARTBEAT message dropped, GR30 interface send failed
Condition:	Third attempt to send a HEARTBEAT CDC message over a GR30 connection failed.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	IAP times out waiting for login digits
Condition:	Law enforcement collection facility for GR30 CDC Dial Out didn't respond with GR30 login digits in the specified time.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	Low
Action to be considered:	Contact LEA personnel.

Error type:	Invalid IP route
Condition:	The IP route destination for an incoming IP datagram is not associated with a CALEA IP interface. The CALEA TCP/IP Security Enhancement feature discarded the incoming IP datagram.
Sensitive CALEA Data:	None
Potential Impact:	Unauthorized access to a switch processor (SMP or PH) via CALEA IP interface was detected. If the unauthorized activity continues, the CALEA IP interface will be removed from service. Valid CALEA CDC/PDC data delivery will be impacted if no other IP interface is available for the destination IP address.
Priority :	High
Action to be considered:	Verify IP network for security breach or misconfiguration.

Error type:	Invalid LOGIN digits received
Condition:	Law enforcement collection facility for GR30 CDC Dial Out responded with invalid GR30 login digits.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	Low
Action to be considered:	Contact LEA personnel.

Error type:	Invalid Protocol Handler CAL_INFO attribute value.
Condition:	Could not find a case ID from CAL_INFO for a packet subject.
Sensitive CALEA Data:	Call Content in X.25 Packet format.
Potential Impact:	Missing call content of the packet subject.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	IP datagram fragment received
Condition:	An IP datagram fragment received on a CALEA IP interface was detected. The CALEA TCP/IP Security Enhancement feature discarded the incoming IP datagram fragment.
Sensitive CALEA Data:	None
Potential Impact:	A potential security breach was detected on a CALEA IP interface. If the unauthorized activity continues, the CALEA IP interface will be removed from service. Valid CALEA CDC/PDC data delivery will be impacted if no other IP interface is available for the destination IP address.
Priority :	High
Action to be considered:	Verify IP network for security breach or misconfiguration.

Error type:	LOGIN message dropped, GR30 interface send failed
Condition:	Third attempt to send a LOGIN CDC message over a GR30 connection failed.
Sensitive CALEA Data:	None.
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	LOGIN Successful
Condition:	Law enforcement collection facility for GR30 CDC Dial Out responded with valid GR30 login digits.
Sensitive CALEA Data:	None
Potential Impact:	None
Priority :	N/A
Action to be considered:	None

Error type:	No FSK or UTD resources available for GR30 interface
Condition:	Attempt to establish GR30 CDC dial out connection failed because no FSK resources were available.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specific GR30.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	No IP route.
Condition:	There is no IP routing information available for the incoming IP packet. The CALEA TCP/IP Security Enhancement feature detected and discarded an incoming IP packet datagram that is not a response to switch-generated IP data.
Sensitive CALEA Data:	None.
Potential Impact:	Unauthorized access to a switch processor (SMP or PH) via CALEA IP interface was detected. If the unauthorized activity continues, the CALEA IP interface will be removed from service. Valid CALEA CDC/PDC data delivery will be impacted if no other IP interface is available for the destination IP address.
Priority :	High
Action to be considered:	Verify IP network for security breach or misconfiguration.

Error type:	No Tone Decoder Available
Condition:	Cannot allocate a tone decoder.
Sensitive CALEA Data:	None
Potential Impact:	No Dialed Digit Extraction CDC message can be sent.
Priority :	High
Action to be considered:	Notify switch maintenance personnel. Additional tone decoders may need to be provisioned in the office.

Error type:	PDC collection facility IP address not obtained.
Condition:	Cannot determine which IP address and port to be sued for a packet level II subject.
Sensitive CALEA Data:	None
Potential Impact:	No call content is sent and the intercepted call is handled as as a level I subject.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	PSLAESCASE tuple missing when adding new monitoring station.
Condition:	PSLAESCASE tuple is not available for a packet subject.
Sensitive CALEA Data:	Party identifier (party member number): Either B1, B2, or D channel, and channel number.
Potential Impact:	Call content for the packet subject may not be available.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Protocol Handler Resource CAL_INFO Exhaustion
Condition:	None
Sensitive CALEA Data:	Party identifier: Either B1, B2, or D member.
Potential Impact:	Party identifier: Either B1, B2, or D member
Priority :	High
Action to be considered:	The SRE RC view can be used to insert more RLCAL_INFO tuples in the affected SMs.

Error type:	RLCASE_IDX data inconsistency
Condition:	Could not find a matching LAES case ID in relation RLcase_idx for a packet subject.
Sensitive CALEA Data:	None
Potential Impact:	Missing packet data channel as IP address cannot be obtained
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLCASE_IDX tuple missing.
Condition:	Could not find the expected tuple in relation RLCASE_IDX.
Sensitive CALEA Data:	None
Potential Impact:	Missing CCC and/or CDC.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLEQUIPDSL tuple missing
Condition:	Could not find the expected tuple in relation RLEQUIPDSL.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specified tuple.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLFC_LINE tuple missing
Condition:	Could not find the expected tuple in relation RLFC_LINE.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specified tuple.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLGR30INTF tuple missing
Condition:	Could not find the expected tuple in relation RLGR30INTF.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specified tuple.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLLAESCASE tuple missing.
Condition:	Could not find the expected tuple in relation RLLAESCASE.
Sensitive CALEA Data:	None
Potential Impact:	Missing CCC and/or CDC.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLLAESPROF tuple missing.
Condition:	Could not find the expected tuple in relation RLLAESPROF.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC messages.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLOFFICECODE tuple missing
Condition:	Could not find the expected tuple in relation RLOFFICECODE.
Sensitive CALEA Data:	None
Potential Impact:	Subject's DN is not outpulsed at end of call content when using CCC Dial Out.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLPORTLA tuple missing
Condition:	Could not find the expected tuple in relation RLPORTLA.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using specified tuple.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLPR_DNTRAN tuple missing
Condition:	Could not find the expected tuple in relation RLPR_DNTRAN.
Sensitive CALEA Data:	None
Potential Impact:	Missing CDC data for surveillance(s) using Local LEA CDC DN.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLRTDNMOD tuple missing
Condition:	Could not find the expected tuple in relation RLRTDNMOD.
Sensitive CALEA Data:	None
Potential Impact:	Missing CCC or CDC data.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	RLRT_DNTRAN tuple missing

Condition:	Could not find the expected tuple in relation RLRT_DNTRAN.
Sensitive CALEA Data:	None
Potential Impact:	Call content is not provided to law enforcement for surveillance(s) requiring DN in RLRT_DNTRAN tuple.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Resource Unavailable.
Condition:	The port for a CCC trunk is not in a valid state.
Sensitive CALEA Data:	None
Potential Impact:	Missing CTONE.
Priority :	High
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Socket not found.
Condition:	Could not find the last connected socket or a connected socket. It occurs when a/the TCP/IP socket used to send CDC data or X.25 packets for a subject's X.25 packet call could not be located.
Sensitive CALEA Data:	None
Potential Impact:	For CDC, another socket will be established. For PDC, subject call content is lost.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

Error type:	Surveillance not started due to SM RLCAL_INFO Exhaustion.
Condition:	Could not allocate RLCAL_INFO for an intercepted subject.
Sensitive CALEA Data:	None
Potential Impact:	CDC and CCC cannot be properly delivered.
Priority :	High
Action to be considered:	The SRE RC view can be used to insert more RLCAL_INFO tuples in the affected SMs.

Error type:	Tone Decoder Dropped.
Condition:	Tone decoder dropped due to other failure/maintenance.
Sensitive CALEA Data:	None
Potential Impact:	Missing DDE CDC message.
Priority :	Low
Action to be considered:	Notify maintenance personnel.

Error type:	Tone Decoder Dropped Due to Load.
Condition:	Tone decoder is dropped, as there is no digit is received after one minute and the tone decoder usage is over the threshold.
Sensitive CALEA Data:	None
Potential Impact:	Missing DDE CDC message.
Priority :	Low
Action to be considered:	No action is required unless LEA wants the DTMF status become essential.

Error type:	Too many IP datagrams received
Condition:	Too many (more than 5 in 10 seconds) TCP/IP datagrams received on a CALEA IP interface had inappropriate data in TCP segment. A TCP/IP segment can only have SYN+ACK, ACK, FIN, FIN+ACK, or RST and no attached data.
Sensitive CALEA Data:	None
Potential Impact:	A potential security breach was detected on a CALEA IP interface. If the unauthorized activity continues, the CALEA IP interface will be removed from service. Valid CALEA CDC/PDC data delivery will be impacted if no other IP interface is available for the destination IP address.
Priority :	High
Action to be considered:	Verify IP network for security breach or misconfiguration.

Error type:	WARNING: GR30 buffered messages will be discarded in 15 minutes
Condition:	Failed to establish the GR30 CDC Dial out connection. 15 minutes before start dumping CDC messages to the CALEA ROP.
Sensitive CALEA Data:	None

Potential Impact:	The CDC messages will be dumped to the CALEA ROP.
Priority :	Low
Action to be considered:	Contact Lucent TSS personnel.

7. RECENT CHANGE VIEWS - CLASS 33

For your convenience, this chapter contains a detailed description of each Class 33 recent change view used by network administrators or others involved in the provisioning tasks for the CALEA feature set.

These views, along with all other recent change views referenced in this information product are also documented in 235-118-25x, *5ESS® Switch Recent Change Reference*. Also, detailed procedures for the general use of the switch's Recent Change interface are documented in 235-118-251, *Recent Change Procedures*.

NOTE: The views contained in this Chapter apply to the 5E15 software release. The 33 class of views were **not** modified for the CALEA application between the 5E14 and 5E15 software releases. View 33.2 was modified in the 5E15 software release due to a non-CALEA feature and is documented appropriately. Please refer to

- 235-118-255, *5ESS® Switch Recent Change Reference — 5E14 Software Release*, for 5E14-specific documentation.
- 235-118-256, *5ESS® Switch Recent Change Reference — 5E15 Software Release*, for 5E15-specific documentation.
- 235-118-257, *5ESS® Switch Recent Change Reference — 5E16.1 Software Release*, for 5E16.1-specific documentation.
- 235-118-258, *5ESS® Switch Recent Change Reference — 5E16.2 Software Release*, for 5E16.2-specific documentation.
- 235-118-259, *5ESS® Switch Recent Change Reference — 5E17.1 Software Release*, for 5E17.1-specific documentation.

33V1 INTERNET PROTOCOL (RC_IPPROC)

Form ID: 33V1
Form Name: RC_IPPROC
View ID: RVIPPROC
Title: INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

1. VIEW DESCRIPTION:

The INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT view (33.1) provides the capability to provision up to five IP addresses and subnet masks, and associated IP, TCP and UDP parameters to a processor (SM or PH).

1.1 VIEW INFORMATION:

SOFTWARE RELEASE = 5E15

OFFICE RECORD(S) = (5987)

ODA FORM NAME = ipproc
ODA FORM TITLE = INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT
ODA OFFICE RECORD(S) = 5987

VIEW PERMISSIONS = RUDI
MAXIMUM TIME OUT = 330

FUNCTION NAME = vipproc

ERROR ID = 660

```
                                        5ESS SWITCH
SCREEN 1 OF 2                         RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

  *1. PROCESSOR ID    ___
  *2. PROCESSOR TYPE  __
(*)3. QUALIFIER 2     ___
(*)4. QUALIFIER 3     ___

          5. IP ADDRESS
ROW LOCAL IP ADDR    IP SUBNET MASK
 1  ___.___.___.___ ___.___.___.___
 2  ___.___.___.___ ___.___.___.___
 3  ___.___.___.___ ___.___.___.___
 4  ___.___.___.___ ___.___.___.___
 5  ___.___.___.___ ___.___.___.___
```

```
                                        5ESS SWITCH
```

```
SCREEN 2 OF 2                          RECENT CHANGE  33.1
(5987)                  INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

IP PARAMETER ASSIGNMENT      UDP PARAMETER ASSIGNMENT
16. REASSEM TIMER ___        23. UDP CHKSUM EN   _
17. ICMP ERR CNT  ___        24. UDP START PORT _____
18. MTU ENABLE    _          25. UDP DEF TTL    ___
19. MTU DISC      _____

TCP PARAMETER ASSIGNMENT
20. TCP MSS         ____
21. TCP START PORT  _____
22. TCP DEF TTL     ___
```

---

2. FIELD DEFINITIONS

* **1. PROCESSOR ID - (PROCESSORID) - (domain IM)** - The ID of the processor. For SM, the SM number. For PH, the number of the SM on which the PH resides.

Domain:
Enter a number from 1 to 192.

Default: no default

* **2. PROCESSOR TYPE - (PROCESSORTYPE) - (domain PRCTP)** - The type of processor.

Domain:
Enter SM or PH.

Default: no default

Form Checks:

If PROCESSORTYPE equals "SM", then do the following:

QUALIFIER2 is set to unspecified.

QUALIFIER3 is set to unspecified.

If PROCESSORTYPE equals "PH", then QUALIFIER2 must be specified.

If PROCESSORTYPE equals "PH", then QUALIFIER3 must be specified.

(*) 3. QUALIFIER 2 - (QUALIFIER2) - (domain I0_254) - Second qualifier of the processor address. For a PH, this field is the PSU community address (COM ADDR) found on RC view 22.2, Packet Switch Unit.

Domain:

For an SM, leave blank. For a PH enter a number from 1 - 254.

Default: no default

Form Checks:

See form check(s) for PROCESSORTYPE.

(*) 4. QUALIFIER 3 - (QUALIFIER3) - (domain QUAL3) - Third qualifier of the processors address.

Domain:
For an SM, leave blank. For a PH, enter PSU SHELF [0-4] (RC view 22.16) and channel group [00-15] (GRP from RC view 22.16).

Default: no default

Form Checks:

See form check(s) for PROCESSORTYPE.

5. IP ADDRESS - (IPADDRESS) - (domain positional list with 5 rows) - IP addresses consisting of a Local IP address and subnet mask. At least one IP address must be specified.

Form Checks:

For every element in the list IPADDRESS do the following:

If IPSUBNETMASK.IPADDR0 is specified, then IPSUBNETMASK.IPADDR0 must equal "255".

If LOCALIPADDR.IPADDR0 is specified, then LOCALIPADDR.IPADDR0 must be in {"001" thru "126", "128" thru "223"}.

On IPADDRESS element, do the following:

If LOCALIPADDR is specified, then IPSUBNETMASK must be specified.

If IPSUBNETMASK is specified, then LOCALIPADDR must be specified.

If LOCALIPADDR is specified, then LOCALIPADDR.IPADDR0 concatenated with LOCALIPADDR.IPADDR1 concatenated with LOCALIPADDR.IPADDR2 concatenated with LOCALIPADDR.IPADDR3 must be in {"001000000001" thru "126255255254", "128001000001" thru "191254255254", "192000001001" thru "223255254254"}.

If LOCALIPADDR.IPADDR0 is in {"001" thru "126"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255000000000", "255192000000" thru "255255255000"}.

LOCALIPADDR.IPADDR1 concatenated with LOCALIPADDR.IPADDR2 concatenated with LOCALIPADDR.IPADDR3 must not be in {"000000000", "255255255"}.

If LOCALIPADDR.IPADDR0 is in {"128" thru "191"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255000000", "255255192000" thru "255255255000"}.

LOCALIPADDR.IPADDR2 concatenated with LOCALIPADDR.IPADDR3 must not be in {"000000", "255255"}.

If LOCALIPADDR.IPADDR0 is in {"192" thru "223"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255255000", "255255255192" thru "255255255240"}.

LOCALIPADDR.IPADDR3 must not be in {"000", "255"}.

See form check(s) for IPADDRESS.LOCALIPADDR.

LOCAL IP ADDR - (IPADDRESS.LOCALIPADDR) - (structure domain CIPADDR) - Local IP address which is to be assigned to the processor.

Domain:
For Local IP address set 1, enter 0 - 126 for Class A, 128 - 191 for Class B, or 192 - 223 for Class C. For Local IP address set 2, 3, and 4, enter 0 - 255.

Form Checks:

The count of elements of {select LOCALIPADDR from IPADDRESS} must be greater than 0.

{Select LOCALIPADDR from IPADDRESS} must be a unique set.

- (IPADDRESS.LOCALIPADDR.IPADDR0) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.LOCALIPADDR.IPADDR1) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.LOCALIPADDR.IPADDR2) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.LOCALIPADDR.IPADDR3) - (domain C0_255RZ) - .

Default: no default

IP SUBNET MASK - (IPADDRESS.IPSUBNETMASK) - (structure domain CIPADDR) - IP subnet mask to be assigned to the processor.

Domain:

Blank, or enter 255 for IP subnet mask set 1. Blank, or enter 0 - 255 for IP subnet mask set 2, 3, and 4.

- (IPADDRESS.IPSUBNETMASK.IPADDR0) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.IPSUBNETMASK.IPADDR1) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.IPSUBNETMASK.IPADDR2) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.IPSUBNETMASK.IPADDR3) - (domain C0_255RZ) - .

Default: no default

16. REASSEM TIMER - (REASSEMTIMER) - (domain I1_255) - Time in seconds that the processor waits to process a packet.

Domain:
Enter 1 to 255 seconds

Default: default = 60

17. ICMP ERR CNT - (ICMPERRCNT) - (domain I20_255) - Number of bytes returned in internet control message protocol (ICMP) error reporting message for this processor.

Domain:
Enter 20 to 255 bytes.

Default: default = 64

18. MTU ENABLE - (MTUENABLE) - (domain BOOL) - Flag to indicate whether the maximum transmission unit discovery algorithm is enabled.

Domain:
Enter Y for yes or N for no.

Default: default = N

19. MTU DISC - (MTUDISC) - (domain I10_10000) - Interval in seconds at which the path maximum transmission unit (MTU) discovery algorithm tries to increase the MTU.

Domain:
Enter 10 to 10000 seconds.

Default: default = 30

20. TCP MSS - (TCPMSS) - (domain I108_8000) - The maximum segment size for the transmission control protocol in bytes.

Domain:

Enter 108 to 8000 bytes.

Default: default = 536

21. TCP START PORT - (TCPSTARTPORT) - (domain I32768_65535) - Lowest automatically allocated (ephemeral) port number for a transmission control protocol connection. Modifying the TCP Start Port field may result in the tear down of any/all currently existing sockets.

Domain:
Enter a number from 32768 to 65535.

Default: default = 49152

Form Checks:

If the database operation equals "U", then TCPSTARTPORT must equal OLDTCPPORT, otherwise the following warning will be issued: "Updating the TCP starting ephemeral port may reset existing TCP connections using this processor."

See form check(s) for IPADDRESS.LOCALIPADDR.

22. TCP DEF TTL - (TCPDEFTTL) - (domain I1_255) - The number of intermediate hops a packet can make before being discarded (one hop is assumed to take one second).

Domain:
Enter 1 to 255.

Default: default = 255

23. UDP CHKSUM EN - (UDPCHKSUMEN) - (domain BOOL) - Flag to indicate if the datagram protocol checksum option is enabled.

Domain:
Enter Y for yes or N for no.

Default: default = Y

24. UDP START PORT - (UDPSTARTPORT) - (domain I32768_65535) - Lowest automatically allocated (ephemeral) port number for a datagram protocol connection. Modifying the UDP Start Port field may result in the tear down of any/all currently existing sockets.

Domain:
Enter a number from 32768 to 65535.

Default: default = 49152

Form Checks:

If the database operation equals "U", then UDPSTARTPORT must equal OLDUDPPORT, otherwise the following warning will be issued: "Updating the UDP starting ephemeral port may reset existing UDP connections using this processor."

See form check(s) for IPADDRESS.LOCALIPADDR.

25. UDP DEF TTL - (UDPDEFTTL) - (domain l1_255) - The number of intermediate hops a packet can make before being discarded (one hop is assumed to take one second).

Domain:
Enter 1 to 255.

Default: default = 255

3. TRIGGER FUNCTIONS

BASE RELATION = TRIGGER FUNCTION (PERMISSIONS)

RLIPTOPCR = PSiptopcr (iud)
RLPCRTOIP = PSpcrtoip (ud)
RLPROTPARM = PSprotparm (iud)

4. BASE RELATIONS

(PERMISSIONS) BASE RELATION — DISTRIBUTION

(r) RLDSLGDATA — FP
(r) RLMODATT — LR
(r) RLPSUSM — LRFP
(u) RLIPADRLOC — FR
(u) RLIPTOPCR — FR
(u) RLLOCIPADR — LP
(u) RLPCRTOIP — FR
(u) RLPROTPARM — FP
(u) RLRC_HOLE — LP
(u) RLRC_QIDX — LP

33V2 INTERNET PROTOCOL (RC_IPINTF)

Form ID: 33V2
Form Name: RC_IPINTF
View ID: RVIPINTF
Title: INTERNET PROTOCOL (IP) INTERFACE ASSIGNMENT

1. VIEW DESCRIPTION:

The INTERNET PROTOCOL (IP) INTERFACE ASSIGNMENT view (33.2) provides the capability to provision up to five IP addresses and subnet masks, and associated IP parameters to an internet interface. View may be keyed by:

- PKT TN and LCN
- PKT MLHG, PKT MEMB and LCN
- TGN, TGN MEMB and LCN
- OE, ISCN and LCN

1.1 CHANGES THIS RELEASE:

- The allowed range of multiline hunt group was increased from 1 - 2000 to 1 - 8191 for the Multiline Hunt Group Capacity Expansion feature. This feature was first made available in the 5E15 software release.

1.2 VIEW INFORMATION:

SOFTWARE RELEASE = 5E15

OFFICE RECORD(S) = (5988)

ODA FORM NAME = ipintf
ODA FORM TITLE = INTERNET PROTOCOL (IP) INTERFACE ASSIGNMENT
ODA OFFICE RECORD(S) = 5988

VIEW PERMISSIONS = RUDI
MAXIMUM TIME OUT = 330

FUNCTION NAME = vipintf

ERROR ID = 831

```
                                    5ESS SWITCH
                                  RECENT CHANGE  33.2
(5988)              INTERNET PROTOCOL (IP) INTERFACE ASSIGNMENT

(*)1. PKT TN          __________                    12. IP ADDRESS
(*)2. PKT MLHG        ____                  ROW GATEWAY IP ADDR IP SUBNET MASK
```



```
(*)3. PKT MEMB          ____                1  ___.___.___.___ ___.___.___.___
(*)4. TGN               ____                2  ___.___.___.___ ___.___.___.___
(*)5. TGN MEMB          __                  3  ___.___.___.___ ___.___.___.___
(*)6. OE                _ ____________      4  ___.___.___.___ ___.___.___.___
(*)9. ISCN              ______              5  ___.___.___.___ ___.___.___.___
 *10. LCN               ___
 #11. INTERFACE NAME    ____________________   23. MCAST ADDR   ___.___.___.___
                                               28. MTU SIZE     ____
                                               29. CALEA IN USE _
```

2. FIELD DEFINITIONS

(*) 1. PKT TN - (PKTTN) - (domain PKTTN) - Packet switching telephone number that can either be an individual packet TN on a DSL (PPB1 or PPB2) or an XAT TN.

Domain:
Enter a 7 or 10 digit telephone number of the form NXXXXXX or NXXNXXXXXX, where N is a number from 2 to 9 and X is a number from 0 to 9.

Interactions: This PKT TN must be provisioned with a destination facility type (FCL TYPE) of INET on View 23.11.

Default: no default

Form Checks:

(PKTTN must be specified and PKTMLHG must be unspecified and PKTMEMB must be unspecified and TGN must be unspecified and TGNMEMB must be unspecified and OE must be unspecified and ISCN must be unspecified) or (PKTMLHG must be specified and PKTMEMB must be specified and PKTTN must be unspecified and TGN must be unspecified and TGNMEMB must be unspecified and OE must be unspecified and ISCN must be unspecified) or (TGN must be specified and TGNMEMB must be specified and PKTTN must be unspecified and PKTMLHG must be unspecified and PKTMEMB must be unspecified and OE must be unspecified and ISCN must be unspecified) or (OE must be specified and ISCN must be specified and PKTTN must be unspecified and PKTMLHG must be unspecified and PKTMEMB must be unspecified and TGN must be unspecified and TGNMEMB must be unspecified).

(*) 2. PKT MLHG - (PKTMLHG) - (domain MLHG) - This field specifies the group number for a packet switching multiline hunt group.

Domain:
Blank, or enter a number from 1 to 8191.

Interactions: This PKT MLHG and member must be provisioned with a destination facility type (FCL TYPE) of INET on View 23.11.

Default: no default

Form Checks:

See form check(s) for PKTTN.

(*) 3. PKT MEMB - (PKTMEMB) - (domain MEMBR1) - This field specifies the number of a particular member within the specified packet switching multiline hunt group. The PKT MLHG and PKT MEMB combination can either be an individual packet service on a DSL (PPB1 or PPB2) or an XAT.

Domain:
Enter a number from 1 to 2015.

Interactions: This PKT MEMB and group must be provisioned with a destination facility type (FCL TYPE) of INET on View 23.11.

Default: no default

Form Checks:

See form check(s) for PKTTN.

(*) 4. TGN - (TGN) - (domain TRKGRP1) - This field specifies the group number for the trunk associated with the IP interface.

Domain:
Enter a number from 1 to 4000.

Interactions: This field can only be greater than 2000 when the Increased Number of Trunk Groups (SFID 172) feature has been purchased using the Secured Feature Upgrade view (8.22). This TGN and member must be provisioned with a destination facility type (FCL TYPE) of INET on view 5.5.

Default: no default

Form Checks:

See form check(s) for PKTTN.

(*) 5. TGN MEMB - (TGNMEMB) - (domain X75PMEMB) - This field specifies the number of a particular trunk member within the specified trunk group.

Domain:
Enter a number from 0 to 23.

Interactions: This TGN MEMB and TGN must be provisioned with a destination facility type (FCL TYPE) of INET on View 5.5

Default: no default

Form Checks:

See form check(s) for PKTTN.

(*) 6. OE - (OE) - (structure domain DSLXATOE) - Enter one alphabetic character followed by an equipment number of the following format:

Form Checks:

See form check(s) for PKTTN.

- (OE.LCENTYPE) - (domain DSLXATOETY) - Office equipment line card equipment type.

Domain:
Enter A, D, E, G, I, K, N, or O where:

Where:

A =	INEN [Integrated Digital Loop Carrier (IDLC) Network Equipment Number].
D =	DEN [Digital Line Trunk Unit Equipment Number].
E =	AIUEN [Digital (U Circuit) Access Interface Unit (AIU) Equipment Number].
G =	GEN [GAMA-Integrated Digital Carrier Unit (IDCU) Equipment Number].
I =	ISDN [Digital (U & T Card) Integrated Services Line Unit (ISLU) Equipment Number].
K =	LCKEN [Digital (T & U Circuit) Integrated Services Line Unit 2 (ISLU2) Equipment Number].
N =	NEN [Digital Networking Unit - SONET (DNU-S) Equipment Number].
O =	OIUEN [Optical Interface Unit Equipment Number]

Default: no default

- (OE.LCEN) - (domain LEN) - Office equipment line card equipment number.

Domain:
For INEN [Integrated Digital Loop Carrier (IDLC) Network Equipment Number], enter (1-192) (0-7) (01-99) (0001-2048) where:

Where:

(1-192) =	SM (Switching Module)
(0-7) =	DNUS (Digital Networking Unit - SONET)
(01-99) =	RT (Remote Terminal)
(0001-2048) =	LINE (Remote Line)

For DEN [Digital Trunk Equipment Number], enter (1-192) (0-5) (01-10) (01-48) where:

Where:

(1-192) =	SM (Switching Module)
(0-5) =	DLTU (Digital Line Trunk Unit)
(01-10) =	DFI (Digital Facility Interface)
(01-48) =	DCHAN (Digital Channel)

For AIUEN [Digital (U Circuit) Access Interface Unit Equipment Number], enter (1-192) (000-104) (00-19) (00-15) where:

Where:

(1-192) =	SM (Switching Module)
(000-104) =	AIU (Access Interface Unit)
(00-19) =	PACK (Pack number)
(00-15) =	CKT (Circuit number)

For RT GEN [GAMA-Integrated Digital Carrier Unit (IDCU) Equipment Number], enter (1-192) (00-42) (01-31) (0001-2048) where:

Where:

(1-192) =	SM (Switching Module)
(00-42) =	IDCU (Integrated Digital Carrier Unit)
(01-31) =	RT (Remote Terminal)
(0001-2048) =	LINE (Remote Line)

For ISDN [Digital (U & T Card) Integrated Services Line Unit (ISLU) Equipment Number], enter (1-192) (0-7) (00-15) (00-31) where:

Where:

(001-192) =	SM (Switching Module)
(0-7) =	ISLU (Integrated Services Line Unit)
(00-15) =	LGC (Line Group Card)
(00-31) =	LC (Line Card)

For LCKEN [Digital (T & U Circuit) Integrated Services Line Unit 2 (ISLU2) Equipment Number], enter (1-192) (00-42) (00-15) (0-7) (00-07) where:

Where:

(1-192) =	SM (Switching Module)
(00-42) =	ISLU2 (Integrated Services Line Unit Two)
(00-15) =	LGC (Line Group Card)
(0-7) =	L Board (Line Board).
(00-07) =	L Circuit (Line Circuit)

For NEN [Digital Networking Unit - SONET (DNU-S) Equipment Number], enter (1-192) (0-7) (0-1) (0-5) (01-28) (01-24) where:

Where:

(1-192) =	SM (Switching Module)
(0-7) =	DNUS (Digital Networking Unit - SONET)

(0-1) = DG (Data Group)
(0-5) = STS (Synchronous Transport Signal number)
(01-28) = VT (Virtual Tributary)
(01-24) = DS0 (Digital Signal Level 0 channel)

For OUIEN [Optical Interface Unit Equipment Number], enter (000-192) (0-7) (0-9) (1) (1-3) (1-7) (1-4) where:

Where:

(000-192) = SM (Switching Module)
(0-7) = OIU (Optical Interface Unit Number)
(0-1) = PG (Protection Group Number)
(1) = OC-3 (Optical Carrier Level-3 Number)
(1-3) = STS (Synchronous Transport Signal Number)
(1-7) = VTG (Virtual Tributary Group)
(1-4) = VTM (Virtual Tributary Member)
(1-28) = CH (Channel Number)

Default: no default

(*) 9. ISCN - (ISCN) - (domain ISCN) - This field specifies the ISCN to which the address is to be assigned.

Domain:
Enter SU shelf[0-4] CHL group [00-15] PH chan [000-127]

Default: no default

Form Checks:

See form check(s) for PKTTN.

* **10. LCN - (LCN) - (domain LCN1)** - This field defines the Logical Channel Number for the packet switching interface.

Domain:
Enter a number from 1 to 127.

Default: no default

 # 11. INTERFACE NAME - (INTERFACENAME) - (domain INTFNM) - This field specifies the name of the interface.

Domain:
Enter name starting with an alphanumeric character followed by 4 to 18 characters including '.', '_' or '-'.

Default: no default

12. IP ADDRESS - (IPADDRESS) - (domain positional list with 5 rows) - Gateway or interface addresses consisting of an IP address and subnet mask. At least one IP address must be specified.

Form Checks:

For every element in the list IPADDRESS do the following:

If IPSUBNETMASK.IPADDR0 is specified, then IPSUBNETMASK.IPADDR0 must equal 255.

If GATEWAYIPADDR.IPADDR0 is specified, then GATEWAYIPADDR.IPADDR0 must be in {"001" thru "126", "128" thru "223"}.

On IPADDRESS element, do the following:

If GATEWAYIPADDR is specified, then IPSUBNETMASK must be specified.

If IPSUBNETMASK is specified, then GATEWAYIPADDR must be specified.

If GATEWAYIPADDR is specified, then GATEWAYIPADDR.IPADDR0 concatenated with GATEWAYIPADDR.IPADDR1 concatenated with GATEWAYIPADDR.IPADDR2 concatenated with GATEWAYIPADDR.IPADDR3 must be in {"001000000001" thru "126255255254", "128001000001" thru "191254255254", "192000001001" thru "223255254254"}.

If GATEWAYIPADDR.IPADDR0 is in {"001" thru "126"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255000000000", "255192000000" thru "255255255000"}.

GATEWAYIPADDR.IPADDR1 concatenated with GATEWAYIPADDR.IPADDR2 concatenated with GATEWAYIPADDR.IPADDR3 must not be in {"000000000", "255255255"}.

If GATEWAYIPADDR.IPADDR0 is in {"128" thru "191"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255000000", "255255192000" thru "255255255000"}.

GATEWAYIPADDR.IPADDR2 concatenated with GATEWAYIPADDR.IPADDR3 must not be in {"000000", "255255"}.

If GATEWAYIPADDR.IPADDR0 is in {"192" thru "223"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255255000", "255255255192" thru "255255255240"}.

GATEWAYIPADDR.IPADDR3 must not be in {"000", "255"}.

See form check(s) for IPADDRESS.GATEWAYIPADDR.

GATEWAY IP ADDR - (IPADDRESS.GATEWAYIPADDR) - (structure domain CIPADDR) - IP address to be assigned to the interface.

Domain:
For Gateway IP address set 1, enter 001 - 126 for Class A, 128 - 191 for Class B, or 192 - 223 for Class

C. For Gateway IP address set 2, 3, and 4, enter 0 - 255.

Form Checks:

The count of elements of {select GATEWAYIPADDR from IPADDRESS} must be greater than 0.

{Select GATEWAYIPADDR from IPADDRESS} must be a unique set.

- (IPADDRESS.GATEWAYIPADDR.IPADDR0) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.GATEWAYIPADDR.IPADDR1) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.GATEWAYIPADDR.IPADDR2) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.GATEWAYIPADDR.IPADDR3) - (domain C0_255RZ) - .

Default: no default

IP SUBNET MASK - (IPADDRESS.IPSUBNETMASK) - (structure domain CIPADDR) - IP subnet mask to be assigned to the interface.

Domain:
Enter 255 for IP subnet mask set 1. Enter 0 - 255 for IP subnet mask set 2, 3, and 4.

- (IPADDRESS.IPSUBNETMASK.IPADDR0) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.IPSUBNETMASK.IPADDR1) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.IPSUBNETMASK.IPADDR2) - (domain C0_255RZ) - .

Default: no default

- (IPADDRESS.IPSUBNETMASK.IPADDR3) - (domain C0_255RZ) - .

Default: no default

23. MCAST ADDR - (MCASTADDR) - (structure domain CIPADDR) - This field defines the multicast address for the interface.

Domain:
Blank, or enter 224 - 239 for Multicast IP address set 1. Blank, or enter 0 - 255 for Multicast IP address set 2, 3, and 4.

- (MCASTADDR.IPADDR0) - (domain C0_255RZ) - .

Default: no default

Form Checks:

If MCASTADDR.IPADDR0 is specified, then MCASTADDR.IPADDR0 must be in {224 thru 239}.

- (MCASTADDR.IPADDR1) - (domain C0_255RZ) - .

Default: no default

- (MCASTADDR.IPADDR2) - (domain C0_255RZ) - .

Default: no default

- (MCASTADDR.IPADDR3) - (domain C0_255RZ) - .

Default: no default

28. MTU SIZE - (MTUSIZE) - (domain I128_1600) - This field defines the maximum number of bytes per transfer from this interface.

Domain:
Enter 128 to 1600 bytes.

Default: default = 256

29. CALEA IN USE - (CALEAINUSE) - (domain BOOL) - This field indicates if this interface is in use by the CALEA Application.

Domain:
Enter Y for yes or N for no.

Default: default = N

3. TRIGGER FUNCTIONS

BASE RELATION = TRIGGER FUNCTION (PERMISSIONS)

RLIPINTCNF = PSipintcnf (iud)
RLIPRTTAB = PSiprttab (iud)

4. BASE RELATIONS

(PERMISSIONS) BASE RELATION — DISTRIBUTION

(r) RLDSLEQUIP — FP
(r) RLEQUIPDSL — FP
(r) RLPR_DNTRAN — FG

(r) RLPSGP_PRT — LPFPFG
(r) RLPSPVCINF — FP
(r) RLRT_MHG — LPFR
(u) RLINTFNAM — LP
(u) RLIPADRLOC — FR
(u) RLIPINTCNF — FP
(u) RLIPRTTAB — FP
(u) RLLOCIPADR — LP
(u) RLNAMINTF — LP
(u) RLRC_HOLE — LP
(u) RLRC_QIDX — LP

33V3 INTERNET PROTOCOL (RC_IPROUT)

Form ID: 33V3
Form Name: RC_IPROUT
View ID: RVIPROUT
Title: INTERNET PROTOCOL (IP) ROUTING TO INTERFACE

1. VIEW DESCRIPTION:

The INTERNET PROTOCOL (IP) ROUTING TO INTERFACE view (33.3) provides the capability to provision an IP gateway between an external IP destination and a local IP interface.

1.1 VIEW INFORMATION:

SOFTWARE RELEASE = 5E15

OFFICE RECORD(S) = (5989)

ODA FORM NAME = iprout
ODA FORM TITLE = INTERNET PROTOCOL (IP) ROUTING TO INTERFACE
ODA OFFICE RECORD(S) = 5989

VIEW PERMISSIONS = RUDI
MAXIMUM TIME OUT = 330

FUNCTION NAME = viprout

ERROR ID = 832

```
                                        5ESS SWITCH
                                      RECENT CHANGE  33.3
(5989)                  INTERNET PROTOCOL (IP) ROUTING TO INTERFACE

 *1. DEST IP ADDR     ___.___.___.___
 *6. INTERFACE NAME   ____________________
  7. NET OR HOST      ____
  8. IP SUBNET MASK   ___.___.___.___
#13. GATEWAY IP ADDR  ___.___.___.___
 18. ROUTE METRIC     ___
```

---

2. FIELD DEFINITIONS

* **1. DEST IP ADDR - (DESTIPADDR) - (structure domain CIPADDR)** - This field specifies one of the

network or host IP addresses that can be reached via this route.

Domain:
For Destination IP address set 1, enter 001 - 126 for Class A, 128 - 191 for Class B, or 192 - 223 for Class C. For Destination IP address set 2, 3, and 4, enter 0 - 255.

- (DESTIPADDR.IPADDR0) - (domain C0_255RZ) - .

Default: no default

Form Checks:

DESTIPADDR.IPADDR0 must be in {"001" thru "126", "128" thru "223"}.

DESTIPADDR.IPADDR0 concatenated with DESTIPADDR.IPADDR1 concatenated with DESTIPADDR.IPADDR2 concatenated with DESTIPADDR.IPADDR3 must be in {"001000000001" thru "126255255254", "128001000001" thru "191254255254", "192000001001" thru "223255254254"}.

See form check(s) for NETORHOST.

- (DESTIPADDR.IPADDR1) - (domain C0_255RZ) - .

Default: no default

Form Checks:

See form check(s) for DESTIPADDR.IPADDR0.

- (DESTIPADDR.IPADDR2) - (domain C0_255RZ) - .

Default: no default

Form Checks:

See form check(s) for DESTIPADDR.IPADDR0.

- (DESTIPADDR.IPADDR3) - (domain C0_255RZ) - .

Default: no default

Form Checks:

See form check(s) for DESTIPADDR.IPADDR0.

* **6. INTERFACE NAME - (INTERFACENAME) - (domain INTFNM)** - This field assigned on view 33.2 specifies the name of and interface.

Domain:
Enter name starting with an alphanumeric character followed by 4 to 18 characters including '.', '_' or '-'.

Default: no default

7. NET OR HOST - (NETORHOST) - (domain NETHOST) - This field indicates if the destination IP address given is a network or host IP address.

Domain:
Enter NET or HOST.

Default: default = NET

Form Checks:

If NETORHOST equals "NET", then do the following:

If DESTIPADDR.IPADDR0 is in {"001" thru "126"}, then IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255000000000", "255192000000" thru "255255255000"}.

If DESTIPADDR.IPADDR0 is in {"128" thru "191"}, then IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255000000", "255255192000" thru "255255255000"}.

If DESTIPADDR.IPADDR0 is in {"192" thru "223"}, then IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255255000", "255255255192" thru "255255255240"}.

IPSUBNETMASK must be specified.

If NETORHOST equals "HOST", then IPSUBNETMASK must be unspecified.

8. IP SUBNET MASK - (IPSUBNETMASK) - (structure domain CIPADDR) - This field specifies the subnetwork mask associated with the destination IP address.

Domain:
Blank, or enter 255 for IP subnet mask set 1. Blank, or enter 0 - 255 for IP subnet mask set 2, 3, and 4.

Form Checks:

See form check(s) for NETORHOST.

- (IPSUBNETMASK.IPADDR0) - (domain C0_255RZ) - .

Default: no default

Form Checks:

See form check(s) for NETORHOST.

- (IPSUBNETMASK.IPADDR1) - (domain C0_255RZ) - .

Default: no default

Form Checks:

See form check(s) for NETORHOST.

- (IPSUBNETMASK.IPADDR2) - (domain C0_255RZ) - .

Default: no default

Form Checks:

See form check(s) for NETORHOST.

- (IPSUBNETMASK.IPADDR3) - (domain C0_255RZ) - .

Default: no default

Form Checks:

See form check(s) for NETORHOST.

 # 13. GATEWAY IP ADDR - (GATEWAYIPADDR) - (structure domain CIPADDR) - This field specifies the IP address of the gateway through which data is sent to the destination.

Domain:
For Gateway IP address set 1, enter 001 - 126 for Class A, 128 - 191 for Class B, or 192 - 223 for Class C. For Gateway IP address set 2, 3, and 4, enter 0 - 255.

Interactions: The GATEWAY IP ADDR must be assigned to the INTERFACE NAME with View 33.2.

- (GATEWAYIPADDR.IPADDR0) - (domain C0_255RZ) - .

Default: no default

Form Checks:

GATEWAYIPADDR.IPADDR0 concatenated with GATEWAYIPADDR.IPADDR1 concatenated with GATEWAYIPADDR.IPADDR2 concatenated with GATEWAYIPADDR.IPADDR3 must be in {"001000000001" thru "126255255254", "128001000001" thru "191254255254", "192000001001" thru "223255254254"}.

- (GATEWAYIPADDR.IPADDR1) - (domain C0_255RZ) - .

Default: no default

Form Checks:

See form check(s) for GATEWAYIPADDR.IPADDR0.

- (GATEWAYIPADDR.IPADDR2) - (domain C0_255RZ) - .

Default: no default

Form Checks:

See form check(s) for GATEWAYIPADDR.IPADDR0.

- (GATEWAYIPADDR.IPADDR3) - (domain C0_255RZ) - .

Default: no default

Form Checks:

See form check(s) for GATEWAYIPADDR.IPADDR0.

18. ROUTE METRIC - (ROUTEMETRIC) - (domain I1_255) - This field specifies the route metric associated with the routing path. This is use for load balancing in multi-routing.

Domain:
Enter 1 - 255.

Default: default = 1

3. TRIGGER FUNCTIONS

BASE RELATION = TRIGGER FUNCTION (PERMISSIONS)

RLIPRTTAB = PSiprttab (iud)

4. BASE RELATIONS

(PERMISSIONS) BASE RELATION — DISTRIBUTION

(r) RLINTFNAM — LP
(r) RLIPADRLOC — FR
(r) RLLOCIPADR — LP
(r) RLNAMINTF — LP
(u) RLIPRTTAB — FP

GLOSSARY

This section provides acronyms and abbreviations used in this document.

-- --

ACK
Acknowledge

AM
Administrative Module

AP
Attached Processor

ARS
Automatic Route Selection

ASM
Administrative Services Module

BAUTO
BRCS Autoform

BFG
BRCS Feature Group

BMI
Batch Mode Immediate (RC)

BMI
Beginning Of Managed Introduction

BMR
Batch Mode Release

BRCS
Business And Residential Custom Services

BRI
Basic Rate Interface

BRI
Batch-Review Inhibited Relation

BST
Bitmap Salvage Technique

CALEA
Communications Assistance for Law Enforcement Act

CAR
Customer Assistance Request

CCC
Call Content Channel

CDC
Call Data Channel

CM1
Communications Module 1

CM2
Communications Module 2

CMD
Command

CPE
Customer Premises Equipment

CST
Central Standard Time

DB
Database

DB
Database Subsystem

DBM
Database Manager

DBM
Database Mode

DEN
Digital Equipment Number

DISP
Display

DN
Directory Number

DSL
Digital Subscriber Line

DTMF
Dual Tone Multifrequency

ECD
Equipment Configuration Data

ECD
Equipment Configuration Database

FIOP
Flexible Input/Output Processor

FOA
First Office Application

FAC
Facilities

FAC
Facility Administration And Control

FAC
Feature Assignment And Construction

FM
Facilities Management

FM
File Manager

HSM
Host Switching Module

IAP
Intercept Access Point

IGN
Ignore

IM
Immediate Mode (RC)

IM
Input Manual

IM
Input Message

IM
Interface Module (now SM)

IOP
Input/Output Processor

IP
Internet Protocol

ISDN
Integrated Services Digital Network

LASS
Local Area Signaling Services

LAES
Lawfully Authorized Electronic Surveillance

LATA
Local Access And Transport Area

LCC
Line Class Code

LEA
Law Enforcement Agency

LEC
Local Exchange Carrier

LEN
Line Equipment Number

MC
Master Control

MCC
Maintenance (Master) Control Center

MCC
Master Control Console

MLHG
Multi-Line Hunt Group

MML
Man Machine Language

MMRSM
MultiModule Remote Switching Module

MSG
Message

MSG
Message Switch

MTU
Maximum Transmission Unit

NIC
Network Information Center

NOC
Normalized Office Code

NPA
Numbering Plan Area

NSC
Network Service Center

NSC
Network Services Complex

NSC
Network Software Center

NSC
Network Systems Corporation

NXX
Office Code (Part Of Dialed Number)

OA&M
Operations, Administration, And Maintenance

OC
Overload Control

ODA
Office Data (Assembler)

ODA
Office Data Administration System

ODA
Office Database Administrator

ODB
Office Database

ODBE
Office Database Editor

ODD
Office Dependent Data

OE
Office Equipment (OEN)

OFR
Office Records

OKP
Operational Kernel Process

OOS
Out Of Service

OP
Operation

ORIG
Originating

ORM
Optical Remote Module

OS
OSDS Subsystem

OS
Operating System

OS
Operations Support

OS
Operations System

OSPS
Operator Services Position System

OTC
Operating Telephone Company

OTR
Operational Trouble Report

OTR
Operator Trouble Report

PARAM
Parameters

PC
Peripheral Controller

PDC
Packet Data Channel

PF
Printout Follows

PF
Private Facility

PH
Packet Handler

PING
Packet Internet Groper

PSU
Packet Switching Unit

PVC
Permanent Virtual Circuit

RAO
Revenue Accounting Office

RBOC
Regional Bell Operating Company

RC
Recent Change Subsystem

RC/V
Recent Change And Verify

RCOS
Recent Change Operations System

RCV
Recent Change And Verify

REPT
Report

RMAC
Remote Memory Administration Center

RMAS
Recent Change Memory Administration System

RMAS
Remote Memory Access System

RMAS
Remote Memory Administration System

ROP
Read (Receive) Only Printer

ROP
Receive Only Printer

RSM
Remote Switching Module

RTAC
Regional Technical Assistance Center

RTR
Real Time Reliable

SAI
Surveillance Administration Interface

SAS
Surveillance Administration System

SAUTO
Shared Autoform

SCCS
Switching Control Center System

SM
Switching Module

STLWS
Supplementary Trunk And Line Work Station

SU
Software Update

TASC
Telephone Company Administrative Support Capability

TCP/IP
Transmission Control Protocol/Internet Protocol

TG
Translation Guide

TG
Trunk Group

TG-5
5ESS® Switch Translation Guide

TGN
Trunk Group Number

TLWS
Trunk And Line Work Station

TMS
Time Multiplexed Switch

TMS
Transmission Measuring Set

TPKT
Transport Control Protocol Packet

TSP
Telephone Service Provider

TTY
Teletypewriter

UTD
Universal Tone Decoder

V
Verify

VDT
Video Display Terminal

VER
Verify

VFY
Verify

XAT
X.25 Access on a T1

List of Figures

Figure 2-1 : CALEA Network Overview

Figure 2-2 : CALEA Network Diagram

Figure 2-3 : CCC Quick Reference

Figure 3-1 : Switch Administration Task Overview

Figure 3-2 : Surveillance Administration Terminal Installation (SPARC5)

Figure 3-3 : Surveillance Administration Terminal Installation (Ultra)

Figure 3-4 : Surveillance Administration Printer Installation (SPARC5)

Figure 3-5 : Surveillance Administration Printer Installation (ULTRA)

Figure 3-6 : CDC/PDC Network Block Diagram

Figure 3-7 : IP Address Assignment Example

Figure 3-8 : Example of Adding a New Trunk Group and Members (Display 1 of 2)

Figure 3-9 : Example of Adding a New Trunk Group and Members (Display 2 of 2)

Figure 3-10 : Example of Deleting a Member From a Trunk Group

Figure 3-11 : Recent Change View Interactions

List of Tables

Table 3-1 : SPARC5 Terminal Locations

Table 3-2 : Ultra Terminal Locations

Table 3-3 : SPARC5 Terminal Locations

Table 3-4 : Ultra Terminal Locations