

5ESS®-2000 Switch
Common Channel Signaling Service Features Feature Document
5E11 and Later Software Releases

Document: 235-190-120

Issue Date: September 1999

Issue Number: 11.00A

Legal Notice

Copyright ©1999 Lucent Technologies, Inc. All Rights Reserved.

This electronic information product (IP) is protected by the copyright and trade secret laws of the United States and other countries. The complete document may not be reproduced, distributed, or altered in any fashion. Selected sections may be copied or printed with the utilities provided by the viewer software as set forth in the contract between the copyright owner and the licensee to facilitate use by the licensee, but further distribution of the data is prohibited.

For permission to reproduce or distribute, call:

1-800-645-6759 (From inside the continental United States)

1-317-322-6847 (From outside the continental United States).

Notice

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

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

Lucent Technologies is the successor to the business and assets of AT&T Network Systems business unit.

Mandatory Customer Information

Interference Information: Part 15 of FCC Rules - Refer to the 5ESS[®] Switch Product Specification IP.

Trademarks

5ESS is a registered trademark of Lucent Technologies.

4ESS is a trademark of Lucent Technologies.

ANSI is a registered trademark of the American National Standards Institute.

AUTOPLEX is a registered trademark of Lucent Technologies.

Common Language is a registered trademark, and CLEI, CLLI, CLCI, and CLFI are trademarks of Bell Communications Research, Inc.

DATATEL is a registered trademark of GTE Lenkurt.

DEFINITY is a registered trademark of Lucent Technologies.

ESS is a trademark of Lucent Technologies.

INTEL is a registered trademark of Intel Corporation.

Motorola is a registered trademark of Motorola, Inc.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

Warranty

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

Ordering Information

This IP is distributed by the Lucent Technologies Customer Information Center in Indianapolis, Indiana.

The order number for this IP is 235-190-120. To order, call:

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

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

Support Telephone Numbers

Information Product Support Telephone Number: To report errors or ask nontechnical questions about this or other IPs produced by Lucent Technologies, call 1-800-645-6759.

Technical Support Telephone Numbers: For initial technical assistance, call the North American Regional Technical Assistance Center (NARTAC) at 1-800-225-RTAC (1-800-225-7822). For further assistance, call the Customer Technical Assistance Management (CTAM) Center:

1-800-225-4672 (From inside the continental United States)

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

The CTAM center is staffed 24 hours a day, 7 days a week.

Acknowledgment

Developed by Lucent Technologies Customer Training and Information Products.

1. INTRODUCTION

1.1 PURPOSE

This document provides information on the 5ESS®-2000 switch application of Common Channel Signaling (CCS) service features. The information contained in this document applies to the 5E11 and later software releases.

CCS features are supported on all platforms except Operator Services Position System (OSPS), Advanced Services Platform (ASP) Release 0, Software Defined Network (SDN), and Leased Network (LN).

1.2 UPDATE INFORMATION

1.2.1 General

This document is being updated to reflect technical changes for the Common Channel Signaling service features on the 5ESS®-2000 switch supported by 5E11 and later software releases:

- 97-CP-4246.K (5E14) - SS7-PSU Capacity and Routing Enhancements Feature
- 97-CP-4463 (5E14) - PSU2 Direct Software Update Feature
- 97-5E-4286 (5E14) - PH22 Base Feature
- 99-5E-4238 (5E14) - MTP Restart and Processor Outage Procedure
- 99-5E-4302 (5E14) - PH22 SCCS Software Image Support Feature
- 99-5E-4687 (5E14) - Release Link Trunk-Toll Feature

1.2.2 Supported Software Releases

In accordance with the 5ESS®-2000 Switch Software Support Plan, the 5E11 software release is rated Discontinued Availability (DA) as of November 13, 1999. The information supporting 5E11 and earlier is being removed over time, instead of concurrently, from all documentation.

If you are supporting offices that use a software release prior to 5E12 and you have a need for the information that is being removed, retain the associated pages as they are removed from the paper documents, or retain the earlier copy of the CD-ROM.

1.2.3 Terminology

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.

National ISDN is an evolving platform in which new features will continue to be introduced for new revenue

opportunities, improved operational efficiencies, and for support of specific applications. NI 1, NI 2, and NI 3 represent specific features as documented in Bellcore SRs 1937, 2120, and 2457. The industry is migrating to an additional terminology to more specifically denote the availability of National ISDN features: NI 95, NI 96, etc. A feature is included in a specific version (such as, NI 96) if it is available by the switch vendors by the first quarter of the year.

As a result of the World Telecommunications Standardization Conference held March 1-12, 1993, the International Telegraph and Telephone Consultative Committee (CCITT), no longer exists as an organization under the International Telecommunication Union (ITU). According to the ITU, the CCITT is now referred to as the International Telecommunication Union - Telecommunication Standardization Sector (ITU-TS).

For new and revised Recommendations issued by the ITU-TS, the term "CCITT Recommendation X.xxx" will be replaced by the "ITU-T Recommendation X.xxx" designation. For a transition period from 1993 to 1997, if the Recommendation had a previous CCITT designation, the new name will include "(formerly CCITT Recommendation X.xxx)." Names of existing CCITT Recommendations will not change unless revised.

1.3 ORGANIZATION

This document is organized into the following sections:

- **Introduction:** Section 1 describes the content and organization of this document. It also describes the reasons for updates and how to obtain assistance.
- **Signaling System 7 (SS7) Overview:** Section 2 contains descriptions of the CCS network, SS7 protocol and Transaction Capability Application Part (TCAP) protocol as they are used in the 5ESS[®]-2000 switch. Also included are considerations for system implementation, operation, and administration in a 5ESS[®]-2000 switch office.
- **Common Network Interface:** Section 3 covers the description, implementation, operation, and administration of the CNI as a part of the 5ESS[®]-2000 switch.
- **Signaling Links:** Section 4 contains setup information for analog and digital signaling links for use with SS7 protocols.
- **ISDN User Part (ISUP):** Section 5 discusses the Integrated Services digital network User Part (ISUP) feature and addresses the considerations for implementation, operation, and administration of the feature.
- **SS7 Conversion - 1A ESSTM To 5ESS[®]-2000 Switch:** Section 6 covers the procedure for CCS conversion required when a 1A ESSTM switch is replaced with a 5ESS[®]-2000 switch.
- **Trunk Conversion:** Section 7 contains considerations and procedures for converting trunks from per-trunk signaling to CCS.
- **Problem Identification:** Section 8 contains tables and charts used for performing manual diagnostics and locating hardware and software problem areas. Also included are tips for locating troubles in the CNI ring such as manual input controls, circuit pack removal procedures, and how to resolve problems not cleared by automatic processes. This section also provides general procedures for determining the cause of service loss due to CCS network problems.
- **ISDN User-Network Interface and ISUP Interworking:** Section 9 covers the description of the Q.931 user-network interface protocol for Integrated Services Digital Network (ISDN) connections and the interworking with SS7 protocol for interswitch ISDN operations.
- **SS7 ISUP Network Interconnect:** Section 10 contains the SS7 ISUP network interconnect capability provided by the 5ESS[®]-2000 switch.

- **ISUP/TCAP Related Features:** Section 11 provides a description of the 5ESS[®]-2000 switch features that use ISUP or TCAP.
- **SS7 Access on a Packet Switch Unit (PSU) Platform:** Section 12 describes SM-based SS7 signaling in both the 5ESS[®]-2000 switch and 5ESS[®]-2000 switch Very Compact Digital Exchange (VCDX) environments.
- **SS7 - PSU Feature Implementation:** Section 13 contains provisioning procedures for signaling links, trunk routes, the signaling connection control part (SCCP) capability, message transfer part/signaling connection control part (MTP/SCCP) measurements, and the transaction capabilities application part (TCAP) application platform.
- **SS7 - PSU Maintenance Considerations:** Section 14 contains SS7 - PSU problem analysis strategies and problem clearing procedures.
- **Glossary:** The Glossary contains definitions of terms and acronyms used in this document.

1.4 USER FEEDBACK

The producers of this document are constantly striving to improve quality and usability. Please use the enclosed user feedback form (paper information products only) for your comments and to advise us of any errors. If the form is missing or your comments will not fit, you can write to the following address:

Lucent Technologies
Documentation Services
2400 Reynolda Road
Winston-Salem, NC 27106

Please include the issue number and/or date of the document, your complete mailing address, and telephone number. We will answer all correspondence within 30 days, informing you of the disposition of your comments.

You may also call our Documentation HOT LINE if you need an immediate answer to a documentation question. This HOT LINE is not intended to eliminate the use of the user feedback form, but rather to enhance the comment process. The HOTLINE number is **1-800-645-6759** and it is available from 7:30 A.M. to 4:30 P.M. Eastern time. Outside of those hours, the line is served by an answering machine. You can leave a message on the answering machine and someone will return your call the following business day.

Document users who have access to electronic mail facilities may send comments via electronic mail. The electronic address is **hotline5@wrddo.lucent.com**. When sending comments via electronic mail please make sure that the document title, document number, document issue number and/or document date are included in the mail along with the sender's name, phone number, and address.

1.5 DISTRIBUTION

This document is distributed by the Lucent Technologies Customer Information Center in Indianapolis, Indiana. Most operating telephone companies should place orders through their documentation coordinator. Some companies may allow customers to order directly from the Customer Information Center; however, the majority do not. Companies that use documentation coordinators to manage their orders receive a significant discount. If you do not know the name/number of the documentation coordinator for your company, you may call **1-888-LUCENT-8 (1-888-582-3688)** to obtain the name and telephone number.

Customers not represented by a documentation coordinator and Lucent Technologies employees can order the documentation for the 5ESS[®]-2000 switch directly from the Customer Information Center. Proper billing information must be provided. These orders may be mailed to:

Lucent Technologies

Customer Information Center
Order Entry
2855 N. Franklin Road
Indianapolis, IN 46219

Orders may also be called in on **1-888-LUCENT-8 (1-888-582-3688)** within the continental United States and **+1-317-322-6416** from outside the continental United States. Orders may be faxed in on **1-317-322-6484**.

1.6 TECHNICAL ASSISTANCE

Technical assistance for the 5ESS®-2000 switch can be obtained by calling the North American Regional Technical Assistance Center (NARTAC) at **1-800-225-RTAC**. This telephone number is monitored 24 hours a day, 7 days a week. During regular business hours, your call will be answered by your local NARTAC. Outside of normal business hours, all calls will be answered at a centralized technical assistance center where service-affecting problems will be dispatched immediately to your local NARTAC. All other problems will be referred to your local NARTAC on the next regular business day.

1.7 REFERENCES

More information on the SS7 and CCS network operations and maintenance is found in the following Lucent Technologies documents:

- 235-060-110 - *Engineering Procedures*
- 235-070-100 - *Administration and Engineering Guidelines*
- 235-070-100 - *Traffic and Plant Measurements, Appendix 1*
- 235-080-100 - *Translations Guide TG-5*
- 235-100-125 - *System Description*
- 235-105-110 - *System Maintenance Requirements and Tools*
- 235-105-200 - *Precutover and Cutover Procedures*
- 235-105-210 - *Routine Operations and Maintenance Procedures*
- 235-105-220 - *Corrective Maintenance Procedures*
- 235-105-231 - *Hardware Change Procedures - Growth*
- 235-105-331 - *Hardware Change Procedures - Degrowth*
- 235-105-250 - *System Recovery Procedures*
- 235-118-2xx - *Recent Change Procedures*
- 235-118-2xx - *Recent Change Reference*
- 235-190-103 - *Business and Residence Feature Descriptions*
- 235-190-104 - *ISDN Feature Descriptions*
- 235-190-115 - *Local and Toll System Features*

- 235-190-125 - *Advanced Services Platform - Release 0 & 0.1A*
- 235-190-126 - *Advanced Services Platform - Release 0.1B*
- 235-190-130 - *Local Area Signaling Service Features*
- 235-200-110 - *Long Distance Platform Document*
- 235-200-150 - *Distinctive Remote Module User's Guide*
- 235-600-700 - *Input Message Manual*
- 235-600-750 - *Output Message Manual*
- 235-700-100 - *Interface Compatibility Guide*
- 235-900-341 - *National ISDN Basic Rate Interface Specification*
- 235-900-342 - *ISDN Primary Rate Interface Specification*
- 235-900-343 - *Custom ISDN Basic Rate Interface Specification*
- 256-010-100 - *CCS Description*
- 256-010-101 - *CCS Fault Recognition and Recovery*
- 256-010-102 - *CCS Direct Signaling Description*
- 256-015-100 - *SS7 LEC Network Description*
- 256-015-300 - *SS7 LEC Network Operations, Administration, and Maintenance*

NOTE 1: For details on translation forms used in Office Data Administration (ODA) refer to the 235-080-100, *5ESS®-2000 Switch Translation Guide*.

NOTE 2: An "x" or "x"s in the last three positions of a release specific document number indicate the digits that change from release to release. Refer to 235-001-001, *Documentation Description and Ordering Guide* for the document number associated with each software release.

NOTE 3: This document also contains information concerning the 5ESS®-2000 switch Compact Digital Exchange (CDX) and the 5ESS®-2000 switch Very Compact Digital Exchange (VCDX), which are switching systems based on the 5ESS®-2000 switch. This document is a standard 5ESS®-2000 switch document that is also applicable to the CDX and VCDX switching systems. Information applicable only to CDX or VCDX may be found in the following manuals:

- 235-120-010, *5ESS®-2000 Switch Compact Digital Exchange (CDX) Reference Guide*
- 235-120-020, *5ESS®-2000 Switch Compact Digital Exchange (CDX) User's Guide*
- 235-120-120, *5ESS®-2000 Switch Very Compact Digital Exchange (VCDX) User's Guide*

2. SIGNALING SYSTEM 7 (SS7) OVERVIEW

2.1 SIGNALING NETWORK

2.1.1 CCS Network Description

The principle of the Common Channel Signaling (CCS) network is to transmit all the signaling information for a group of trunks over a channel separate from the voice/data communication channels. Figure 2-1 is a simplified typical CCS network configuration.

A simplified illustration of the relationship between the CCS network and the voice/data network is shown in "CCS Network Services," Section 2.1.2 of this manual.

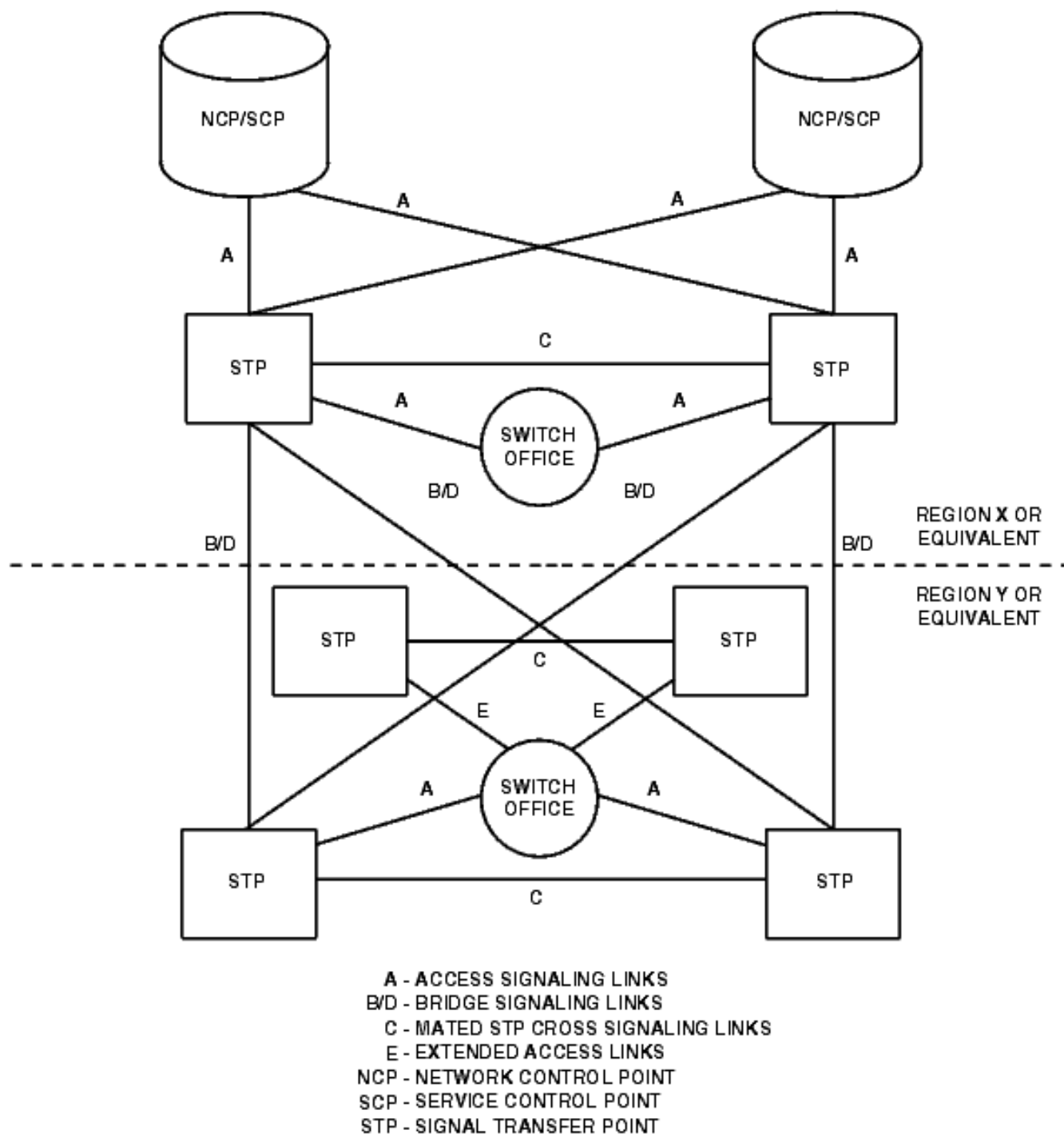


Figure 2-1 A Typical CCS Network Configuration Typical CCS network configuration

2.1.2 CCS Network Services

The CCS network provides out-of-band call control signaling for voice and data telecommunications services. Out-of-band signaling has its own path apart from the voice and data channels for which signaling is being provided. By separating the signaling function from the voice and data transmission path, call completion time is almost 24 times faster and a wider selection of services is available. Figure 2-2 is a simplified illustration of the relationship between the voice/data transmission network and the CCS network.

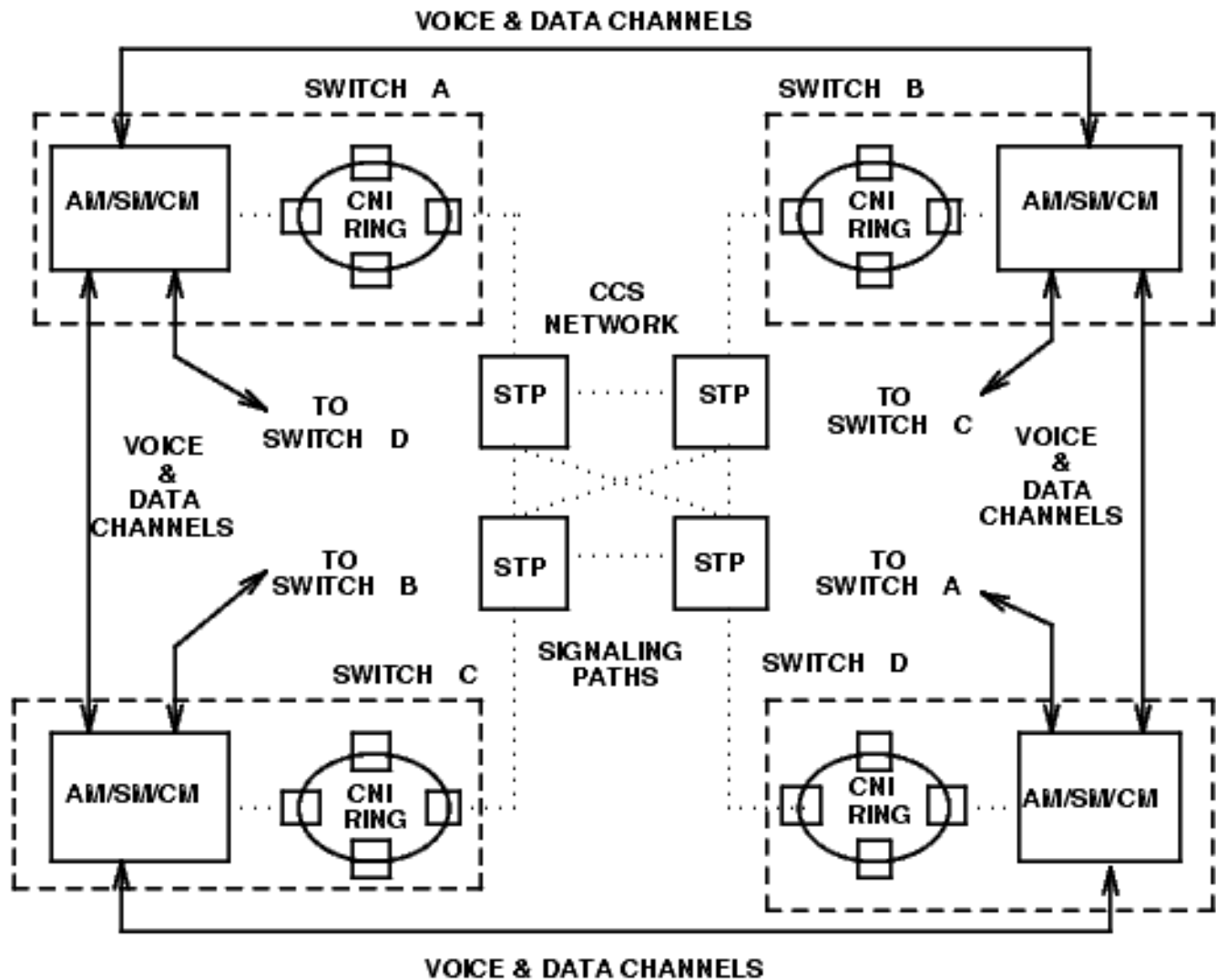


Figure 2-2 Relationship Between the CCS Network and the Voice/Data Network

In addition to the call control signaling, the CCS network provides signaling for querying data bases for information.

The 5ESS[®]-2000 switch uses the CCS network services to:

- Reduce call setup time
- Transfer network management messages
- Provide means of retaining identity of different types of traffic using the same trunk group
- Provide trunk make-busy and other maintenance functions
- Perform other network operations and administration functions
- Provide out-of-band call control signaling for voice and data trunking
- Provide toll-free Service Access Code (SAC) service, such as 800 or 888 numbers

- Provide interface to the Operator Services Position System (OSPS)
- Transport information used by Local Area Signaling Services (LASS)
- Provide access to a service control point to allow the configuration of an advanced services platform on the public-switched network.

The switch accomplishes these functions by combining the signaling information for several channels and transmitting the information over a CCS data link. The signaling information is transmitted by sets of messages between switching processors.

2.1.3 Signal Transfer Point

A Signal Transfer Point (STP) is a general purpose high-capacity packet switch that performs signaling message switching and CCS network management functions. An STP serves as a signaling message switching center, sorting and redirecting signaling messages from incoming signaling links to outgoing signaling links. No signaling link switching is involved, only the transfer of signaling messages. An STP routes signaling messages to and from service control points, other STPs, and end offices.

An STP also performs network management functions by reconfiguring signaling paths using a predetermined strategy for routing signaling messages around failures in the CCS network. Signaling paths are routes through the CCS network composed of one or more signaling links. Signaling route management is accomplished by selectively broadcasting special CCS network management messages to inform switching offices, and other STPs, of changes in the status of signaling paths. In addition to signal route management, selective messages are broadcast to those offices that are affecting a congested switching office to request that those offices reduce the congestion.

Figure 2-3 illustrates the ring type structure used by Lucent Technologies products STPs for interfacing with transmission facilities. The components of the STP are the Administrative Module (AM), link nodes, and ring peripheral controller nodes. A dual ring bus provides access between all nodes. The link nodes provide the interface between the ring and the signaling links, and the ring peripheral controller node interfaces between the ring and the AM.

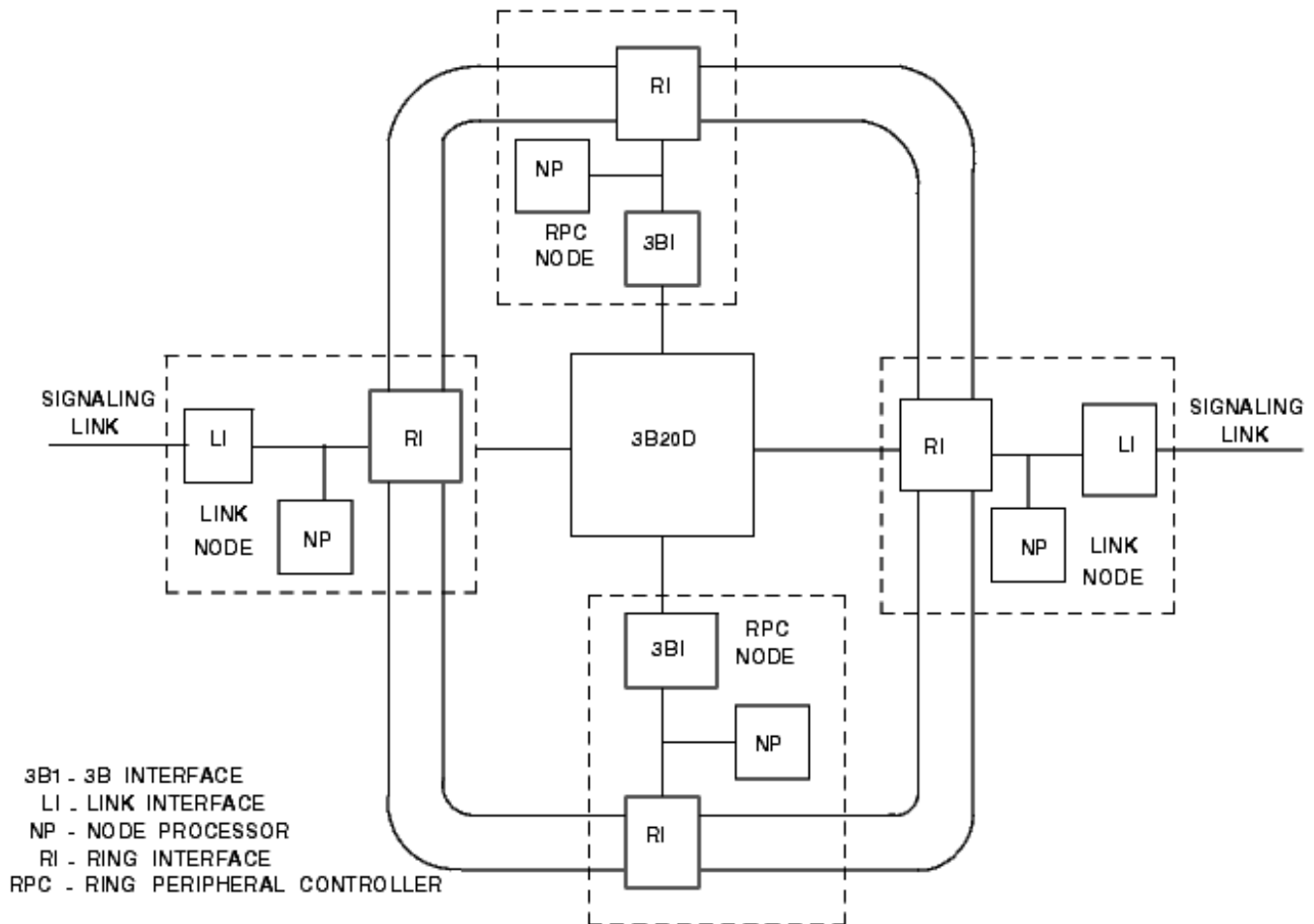


Figure 2-3 Lucent Technologies Products STP Simplified Diagram

2.1.4 Switching Systems

The switching office, or Central Office (CO), is the normal origination or termination of signaling messages. The CO's primary function is to handle telephone calls. It uses the Signaling System No. 7 (SS7) network to provide interswitch services (such service might be the signaling to control a telephone call). Typically, most Signaling Points (SPs) in the network are dispersed over a wide geographical area.

Signaling messages arrive on a signaling link terminated at a link node. The link node determines if the message is to be routed to an outgoing signaling link, or to the AM for additional processing.

2.1.5 Service/Network Control Point

A service control point/network control point is a signaling point in the CCS network containing detailed logic and data used to provide diversified calling services and features. Service related queries from offices in the CCS network are routed to a Service Control Point/Network Control Point (SCP/NCP) where replies are formulated and returned to the originating offices.

2.1.6 Signaling Links

Figure 2-4 illustrates the makeup of a typical signaling link. The signaling link consists of two link nodes that communicate with each other via a signaling link. The function of the signaling link is to transfer CCS signaling

messages between signaling points in the CCS network. Digital signaling links operate at 56 kb/s and support both ECIS and SS7 protocols.

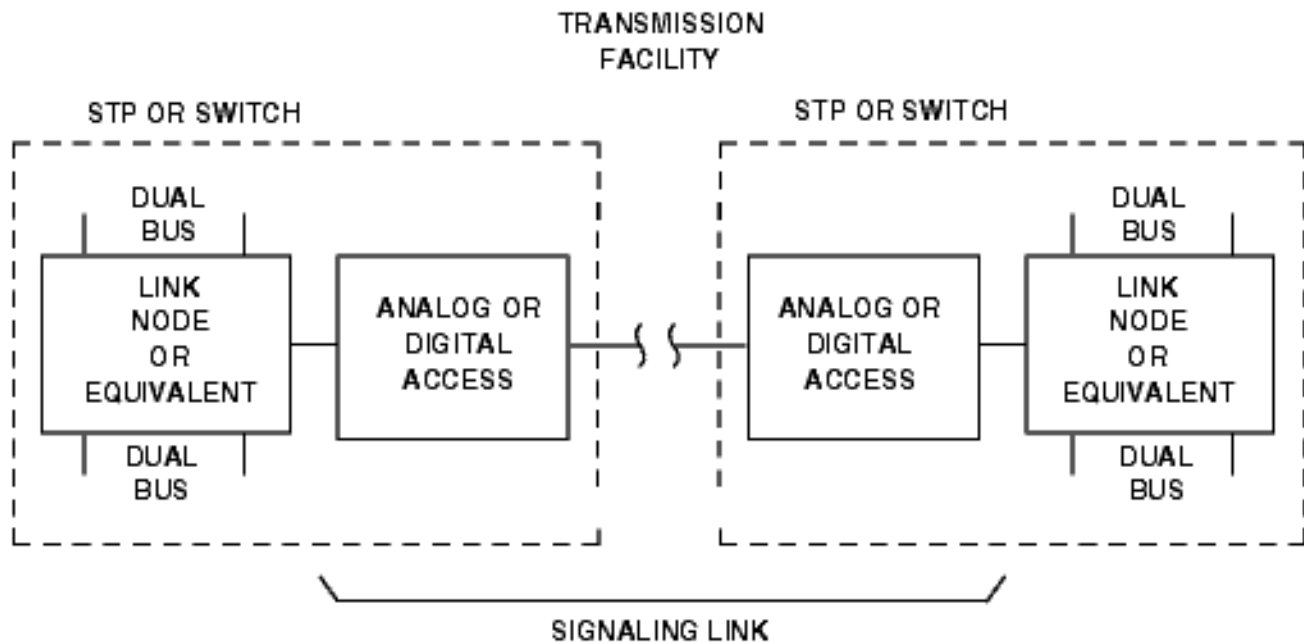


Figure 2-4 CCS Signaling Link

The following types of signaling links are used in the CCS network:

- A-Links -** Access signaling links: The A-link connects the switching office (5ESS®-2000 switch or equivalent) to the CCS network STP.
- B/D-Links -** Bridge signaling links: The B/D-link connects mated pairs of STPs with other mated pairs of STPs in the desired configuration.
- C-Links -** Mated STP cross signaling links: These links connect an STP with its mated STP within the region.
- E-Links -** Extended access signaling links: These links connect the switching office and non-home STPs.
- F-Links -** Direct signaling links: Available in a 5E12 software update, these links directly connect one signaling end point to another.

2.2 SIGNALING PROTOCOL

2.2.1 Signaling Protocol Introduction

The CCS signaling protocol is covered in "SS7 Protocol Definition," Section 2.2.3 .

2.2.2 Implementation

The implementation of the CCS signaling system in a switch office requires the following:

- All features require a properly installed Common Network Interface (CNI) ring.
- The CNI must be connected to an STP pair:

- Signaling links must be set up and properly defined in the data base.
- Network data must be installed (for example, network ID).
- Any switching module on which CCS trunks [ECIS or Integrated Services digital network User Part (ISUP)] terminate must be equipped with a Digital Service Unit model 2 (DSU2).
- The following features (when provided) require activation as a part of the network implementation:
 - SS7 Trunk Signaling
 - SS7 Line Information Data Base (LIDB)
 - SS7 Service Switching Point (SSP) 800 Signaling
 - Local Area Signaling Services (LASS)
 - ECIS Trunk Signaling

2.2.3 SS7 Protocol Definition

The SS7 protocol is defined in accordance with standards established by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-TS), formerly CCITT. The SS7 model is patterned after the seven-layer Open Systems Interconnection model.

Table 2-1 contains an explanation of the seven Open System Interconnection (OSI) protocol layers of the SS7 protocol model.

Table 2-1 SS7 Protocol Description

OSI PROTOCOL LAYER NO.	PROTOCOL LAYER DESCRIPTION	SS7 PROTOCOL LEVEL
Layer 1	Physical Layer - provides transparent transmission of the bit stream over a circuit built in some physical communication medium and furnishes the standard electrical and procedural interface.	MTP
Layer 2	Data Link Layer - assures reliable transmission over the data link by overcoming the limitations inherent in physical circuits and establishes error detection and recovery capability - improving transmission quality and masking deficiencies.	
Layer 3	Network Layer - transfers data transparently between end-users. One or more subnetworks may interwork to provide an end-user to end-user network service. In a connectionless network, the transfer of data between end-users is made with no attempt to guarantee a relationship between two or more data packets from the end-user. The MTP (in SS7), on the other hand, provides the strategies for correctly sequencing the data packets between users.	SCCP
Layer 4	Transport Layer - provides end-user to end-user transfer, optimizing the use of resources (that is, network service) as to the type and character of the communication and relieves the user of concern for transfer details. Sequencing and error control functions help to ensure reliable packet delivery between end-users.	ASP and ISUP (and portion of Layer 3)
Layer 5	Session Layer - manages the connection between communicating application processes. The layer is not required where connectionless service is provided.	
Layer 6	Presentation Layer - transforms the syntax of the transferred data to meet the requirement of the application process.	
Layer 7	Application Layer - establishes an independent end-to-end flow control (peer-to-peer	TCAP

	protocol) for the designated user need.	and OMAP

The SS7 signaling protocol is used for routing and handling messages over the CCS network. A maximum of 272 bytes of data can be transferred in a signaling message. The variable length messages are routed over the CCS network 56 kb/s signaling links using a destination address called a signaling point code. This signaling point code is unique to each signaling point in the SS7 network.

The basic levels of this structure are as follows:

- Message Transfer Part (MTP)
- Signal Connection Control Part (SCCP)
- Integrated Services digital network User Part (ISUP).

2.2.4 Message Transfer Part

2.2.4.1 Message Transfer Part Introduction

The SS7 protocol is a layered protocol; that is, different functional components in the protocol rely on the other components to operate. The SS7 ISUP is used for call control between two or more switching offices. However, ISUP depends on the MTP to deliver the message from one office to the next. The MTP manages the routing of the message through the signaling network using destination point codes. The destination point code identifies each signaling point with a network ID, a cluster number, and member number. The destination point code routing is accomplished by use of message handling, signaling link management, and signaling route management functions.

2.2.4.2 MTP Message Priority

Each message sent from the switch is assigned a message priority value in the Service Information Octet (SIO). These values range from 0 to 3, where 3 is the highest priority and 0 is the lowest priority. The priority value is used by various processors in the network to manage signal message congestion.

A point code table is kept in the switch. Each connecting point code is stored along with its associated congestion level, a value from 0 to 3. A point code congestion level of 1, 2, or 3 means that the far destination is in congestion. A Transfer Control (TFC) message is used to signal congestion to other points in the network. When the switch gets a TFC message, it updates the point code table with the appropriate congestion level.

This table is accessed at two points in the switch — as trunk hunt is attempted from a particular trunk group and prior to each signaling message being sent out of the switch. Trunk hunt will not search for an idle trunk in a trunk group unless the congestion level of the corresponding destination point code is 0 or 1. When a signaling message is sent out of the switch to a particular destination, the message priority is compared with the stored congestion level for its destination point code. The message will go out on the signaling link only if its priority is $\geq$ to the congestion level of the destination point code.

2.2.5 Signaling Connection Control Part

The SCCP provides the MTP with the ability to transfer circuit-related or noncircuit-related messages with a guaranteed in-sequence delivery. It also allows the transfer of other types of information between offices and specialized centers in the telecommunications networks. The SCCP provides logical signal connections within the CCS network and the ability to transfer signaling data with or without these connections. The destination and origination of a message is identified by the called and calling party addresses. Either address may contain a combination of global title, subsystem, and point code.

2.2.6 Message Format

The **SS7 Signaling Message Format** (Figure 2-5) is used for both long distance and Local Exchange Carrier (LEC) CCS networks.

The SS7 signaling message format is variable in length, up to 272 bytes. An example of a SS7 signaling message is shown in Figure 2-5 . This flexible signaling message format eliminates the signal unit and length limitations of the ECIS protocol. The SS7 signaling protocol allows new services to be implemented more efficiently.

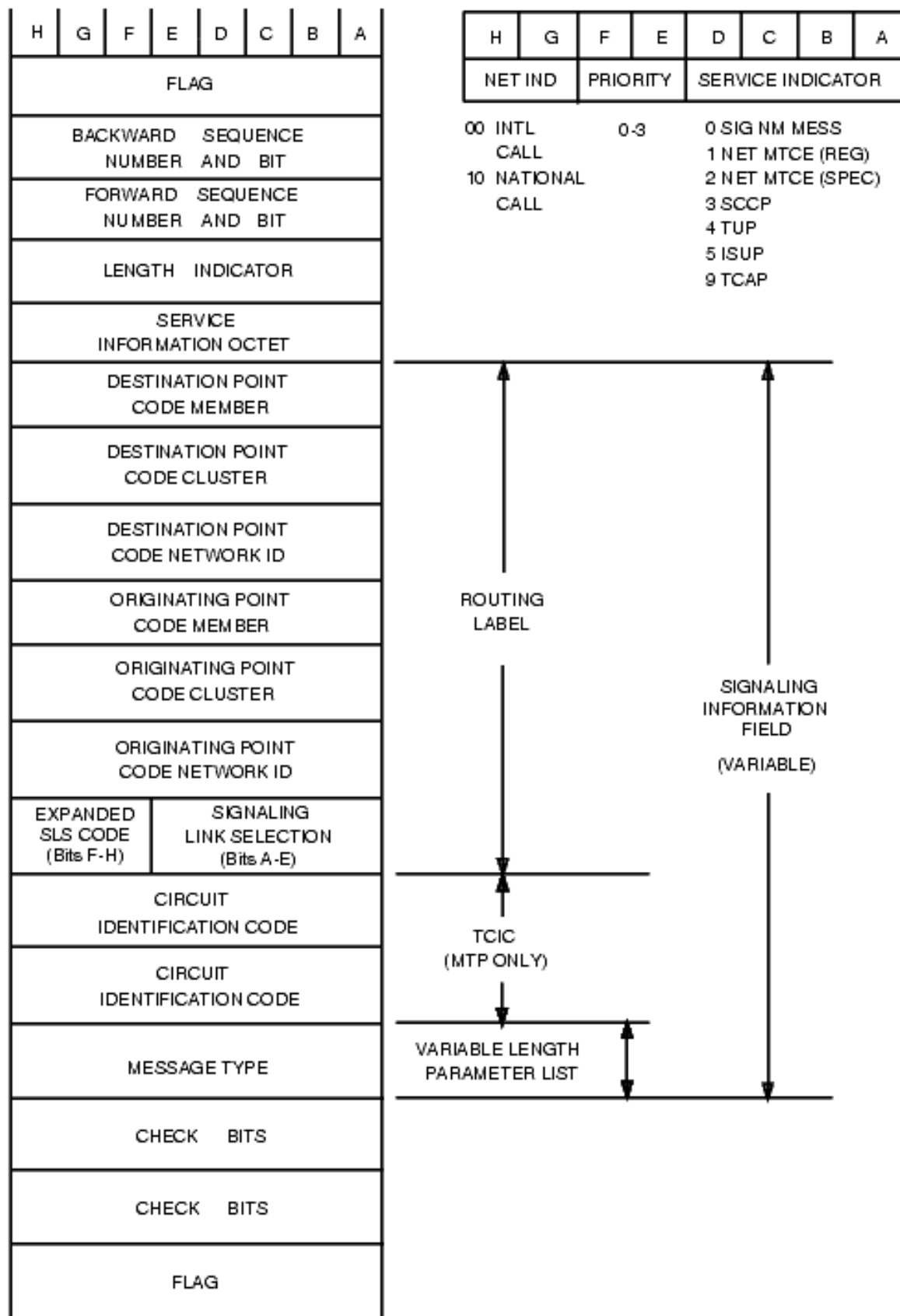


Figure 2-5 SS7 Message Format

2.2.7 Message Routing

2.2.7.1 Message Routing Introduction

The signaling message routing process depends on the STPs in the network as primary switching centers for all message routing. The STPs contain information about routing status, destination point code translations, and global title directory number routing capacity.

Destination Point Code Routing: This 24-bit routing code assigned to every signaling point in the CCS network is the network address for a signaling node. With a known destination point code, the SS7 network can route messages to a node based on its point code.

Global Title Routing: The SCCP directs the signaling message to the appropriate STP for translation. Many translation types can be used to establish the domains for global title addresses. Some of these types can be the toll-free Service Access Code (SAC), dialed number screening, or password validation. The STP translates the global title address to a destination point code and subsystem number. The subsystem number identifies the service at the signaling node for which the message is intended. The network uses the destination point code to complete the routing.

2.2.7.2 Routing Label

The routing label is part of the signaling message used to route the message to a particular destination point. The routing label contains signaling link selection and destination and originating point codes. The routing label is placed in the signaling label field that has 56-bit length.

The signaling link selection (SLS) field, in the routing label, consists of 5 or 8 bits used to distribute the network traffic load between links of the same linkset or a combined linkset. (For a description see "Expanded Signaling Link Selection [SLS] Code," Section 2.3 .

The point code portion of the routing label consists of two 24-bit fields for the destination point code and the originating point codes. Each point code may have three subfields as follows:

- Network ID
- Network cluster
- Cluster member.

2.2.7.3 Trunk Circuit Identification Code

The routing label directs signaling messages between two switching exchanges over a specific circuit group. A circuit identification code is provided to associate the message with a particular circuit.

2.3 EXPANDED SIGNALING LINK SELECTION (SLS) CODE

2.3.1 Feature Description

The Signaling Link Selection (SLS) Code Expansion, feature number 99-CP-2316, expands the current 5 bit SLS code to 8 bits. The value of the Signaling Link Selection (SLS) code determines the links and STPs used to route a message.

This expansion allows the maximum size of a B or D link set to be 16 links, compared to the previous limit of 8. The expansion also allows a more even distribution on links in a "combined" link set, especially after link failures.

This is a secured feature (SFID=175) and a right-to-use (RTU) fee must be paid to Lucent Technologies before enabling information is provided.

2.3.2 Background

The Signaling Network Systems (SNS) Committee of the Federal Communications Commission's (FCC) Network Reliability Council, T1S1.3 provides CCS network architecture evaluations and SS7 protocol enhancements. To facilitate uniform industry deployment a SNS subgroup prioritized enhancements into two levels. This SLS Code Expansion feature is one of the features in the high priority level.

2.3.3 Availability

This feature is distributed in the 5E11 software release.

2.3.4 Feature Environment

This feature is provided per switch.

2.3.5 Feature Operation

The Expanded SLS code feature is compatible with the existing 5 bit SLS code. An 8 bit SLS code can be sent to a STP which uses the 5 bit code, because the STP will just use the 5 least significant bits for routing and will ignore the 3 most significant bits, even if they are non-zero.

After the SLS code is generated and a route is selected, but prior to message transmission, the five least significant bits ($X_4 X_3 X_2 X_1 X_0$) of the 8 bit SLS code are rotated right by one bit (that is, shifting only the five least significant bits one position to the right and placing the first bit into the fifth bit position). To achieve compatibility with the 5 bit SLS scheme, the three most significant bits ($X_7 X_6 X_5$) are not included in the rotation. This is illustrated as follows:

Bits $X_7 X_6 X_5 X_4 X_3 X_2 X_1 X_0$ are rotated to these positions $X_7 X_6 X_5 X_0 X_4 X_3 X_2 X_1$ prior to message transmission

2.3.6 User Operation

Switch personnel will use recent change procedures to enable (unlock) the security and activate the feature.

2.3.7 Engineering

2.3.7.1 Hardware Resources

No hardware considerations are associated with this feature.

2.3.7.2 Software Resources

No software considerations are associated with this feature.

2.3.7.3 Transition Considerations

There are no transition considerations because this feature is compatible with existing SLS codes.

2.3.8 Interactions and Limitations

This feature creates a general security mechanism that is used to secure other CNI-related features.

2.3.9 Incompatibilities

There are no incompatibilities associated with this feature.

2.3.10 Dependencies

No dependencies have been identified.

2.3.11 Isolation Constraints

Not applicable.

2.3.12 Feature Implementation

2.3.12.1 Office Data Administration (ODA) Provisioning

There is no ODA provisioning associated with this feature.

2.3.12.2 Recent Change Provisioning

The service provider must enable (unlock) this secured feature and activate the feature using recent change procedures.

Unlock the security lock for the feature by populating Recent Change view 8.22, *Secured Feature Upgrade*:

FIELD	*VALUES
FEATURE ID	175
MODULE	(Office or SM 1-192)
PASSWD	(Provided by Lucent Technologies)
	(SFID Administrator)
ACTIVE	Y
	"Y" - Turns on (unlocks) the feature
	"N" - Turns off (locks) the feature

Activate the feature using Recent Change view 8.15, *CCS Office Parameters*:

FIELD	*VALUES
EXPANDED_SLS	Y
	"Y" - Turns on (enables) the feature
	"N" - Turns off (disables) the feature

* See 235-118-2xx, 5ESS[®]-2000 Switch Recent Change Reference for detailed information on allowed values.

2.3.13 Administration

This feature does not introduce any new measurements and does not impact billing.

3. COMMON NETWORK INTERFACE

The Common Network Interface (CNI) is a packet-switching system used for switching signaling messages in the Common Channel Signaling (CCS) network. The CNI has a community of peripheral processors in a ring configuration interfaced to a central processor. The 5ESS®-2000 switch Administrative Module (AM) performs the basic duties of the system in controlling the message flow and system operation.

The processors, known as link nodes using Signaling System Number 7 (SS7) protocol, function as routing devices for the messages that are transmitted over the network in byte segments.

This section provides a description of the CNI ring in the switch. There are several CNI configurations discussed that may be used in the switch configuration, depending on the office requirements. Figure 3-1 shows the switch CNI/Interprocess Message Switch (IMS) configuration.

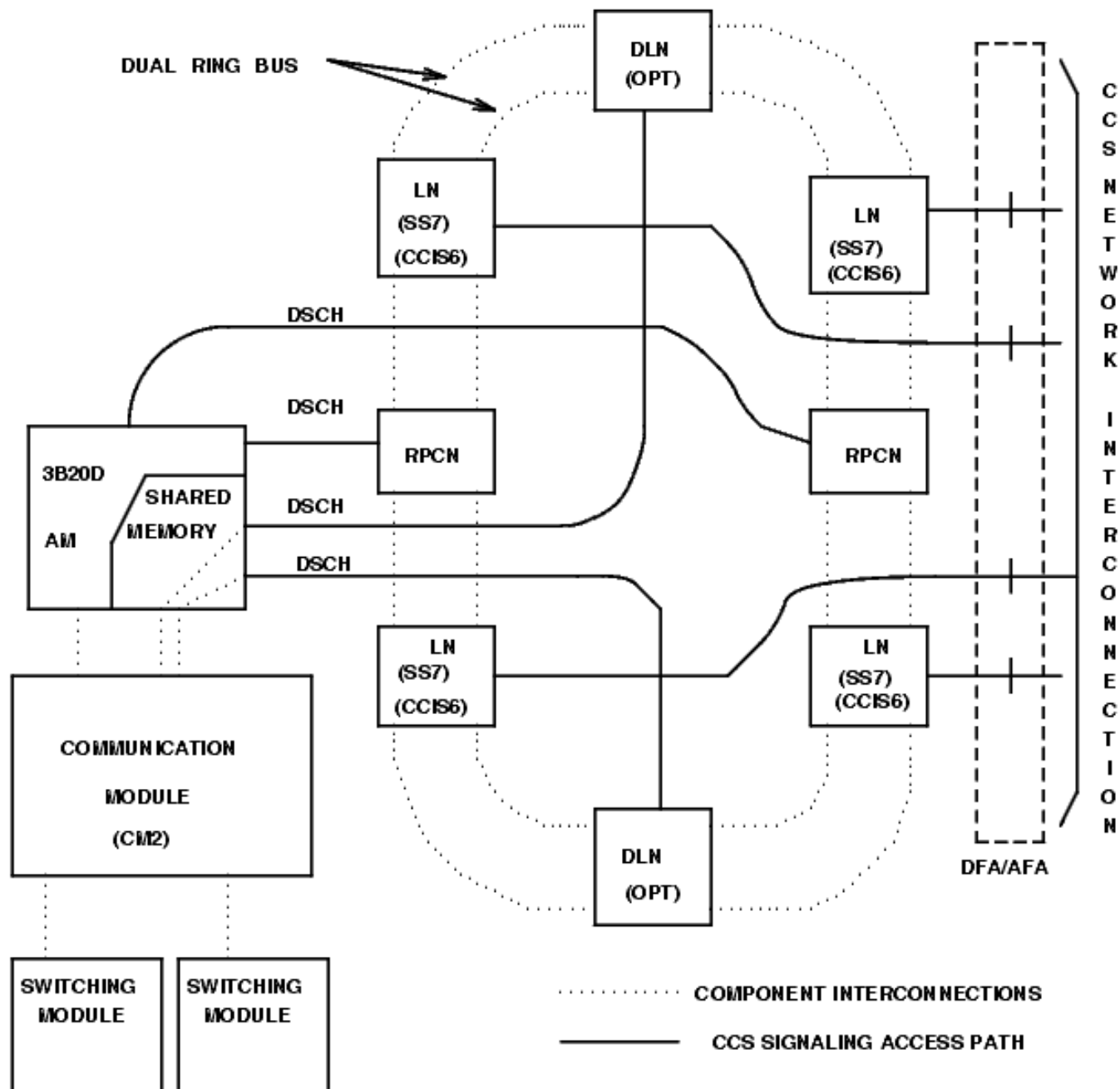


Figure 3-1 5ESS -2000 Switch CNI Configuration

CNI FEATURES

The switch CNI configuration provides the following features:

- CCS message handling capacity
- Termination for 56 kb/s links encrypted or nonencrypted
- Reliable system operation:

- Automatic system recovery following hardware failure.
- Diagnostics that isolate most faults. (See 235-105-220, *Corrective Maintenance Manual* for supplemental information.)
- Processor recovery messages are used to identify processors that may be encountering a failure. These are discussed later in this section and in more detail in 235-600-601, *Processor Recovery Messages Manual*.
- System integrity is maintained during error and overload conditions.
- Manual interfaces for surveillance, control, and maintenance.
- Measurements, reports of performance, and log files are used in maintenance, engineering, and administration of the CNI office. These are generated locally for assembling information to be sent to a remote collection center. The reports can be as follows:
 - Scheduled or demanded
 - For the total office, and specific links
 - Software release defined formats, or user defined flexible formats
 - Real-time notification of CCS network critical events.

See 235-070-100, *Administration and Engineering Guidelines* for other information on IMS and CNI measurements and reports.

- Software and hardware integrity audits:
 - System audits
 - Internal data audits (per link and total office)
 - Neighbor ring node hardware audits
 - Ring silence monitoring.
- Maintenance and fault recovery:
 - Automatic ring recovery program
 - Isolation of faulty ring sections and quarantine of nodes that require maintenance
 - Initialization: If a CNI fault occurs that requires reinitialization, there are four CNI levels and five IMS levels (separate from the AM) under the condition that one does not interrupt normal call processing. The AM initialization level 51 may cause the CNI to initialize; whereas, levels 52 through 54 always cause the CNI to initialize.
 - Diagnostics for nodes and links (automatic and demand)
 - Ring reinitialization, even in presence of failures
 - Congestion controls for the ring, nodes, links, and central processor

— Node Restarts.

CNI NODE TYPES

There are five kinds of CNI nodes available for the switch.

- **Ring Peripheral Controller Node (RPCN):** This node provides communication between the ring and the AM. There is an RPCN placed in position 0 of group 00 and group 32. Two are always used in the switch CNI application.
- **Link Node (LN):** This node provides communication between the CNI ring and the CCS network. The LN speed is 56 kb/s and nonencrypted. From 2 to 38 LNs can be used in the switch CNI application.
- **Interprocess Message Switch User Node (IUN):** This is an active node on the CNI ring, but performs no signaling or processing. One use of the IUN, in the switch application, is to electrically hold a place for a future LN and provide the foundation of common circuitry on which the LNs are built. This avoids ring cabling at the time of growth. The IUN may control an adjacent interframe buffer that is used to connect ring nodes across a physical frame boundary; however, it is generally a temporary filler during growth or reduction periods.
- **Direct Link Node (DLN):** The DLN, an optional node is for switches equipped with Communication Module 2 (CM2). The DLN relieves the AM of some signaling message processing to support greater CCS processing capacity. When DLNs are used, there are always two required for the switch, used in an ACTIVE/STANDBY mode.
- **Direct Link Node 30 (DLN30):** The Direct Link Node 30 (DLN30) provides support for higher CCS7 capacity, which includes ISUP and TCAP applications, on the switch. This capacity increase is accomplished by replacing the Small Scale Integration (SSI) nodes on the CNI ring with the newer technology Integrated Ring Node 2 (IRN2) hardware.

3.1 CNI RING STRUCTURE

3.1.1 CNI Ring Structure Introduction

The CNI ring node frame is a single cabinet. The cabinet includes the power panel, shelves for ring nodes, and a fan unit.

3.1.2 CNI Cabinet

3.1.2.1 CNI Cabinet Introduction

The cabinet is 6 feet 4 inches tall, 2 feet 2 inches wide, and 30 inches deep. It is equipped with doors on the front and back. The rear doors include ventilation openings. The cabinet rests on insulated feet. The CNI is housed in a "2000 switch" cabinet, which is essentially a single bay. The fans are mounted in the middle of this cabinet.

3.1.2.2 Units

Shelf assemblies or units form the basic building blocks for the cabinets. Units are formed from various shelf assembly parts (for example, apparatus mountings, card guides, circuit packs, connectors, and interconnecting wiring).

3.1.2.3 Circuit Packs

Circuit packs are housed in apparatus mountings that have guides to align the circuit pack with the connector pin field at the back of the shelf assembly. The circuit packs within a unit are spaced horizontally across the cabinet with sufficient space between boards to provide equipment cooling.

3.1.2.4 Node To Node Cabling

The CNI nodes are interconnected by a high-speed data bus and a maintenance bus in parallel. The cabling from node-to-node (sometimes through buffer cards) forms the ring. Rings 0 and 1 are independent of each other. Ring 0 is active and Ring 1 is standby. Ring 0 is used for traffic and message handling, while Ring 1 carries internal maintenance messages. The rings propagate data in opposite directions. The nodes are designed so that equipment can be removed when a trouble condition exists. A node can be isolated from Ring 0 without being physically removed, in which case it is electrically separated from the ring. The ring may have an active segment and an isolated segment at the same time. An isolated node can be diagnosed, serviced, and restored without interfering with ring traffic.

3.1.2.5 Ring Node Addressing

Circuit packs used in the CNI ring are interchangeable between nodes. For this reason, the node must find out its particular address from pins grounded on the backplane. The ID pins are a binary representation of the node's address. The value is calculated by the following:

$$(\text{group number}) \times 16 + (\text{member number}) = \text{node's address}$$

An additional ID pin (MPN) must be grounded for RPCNs.

3.1.3 Environment Requirements

3.1.3.1 Heat Dissipation

The integrated circuits used in the circuit packs require that the operating circuit board temperature not exceed 70°C (158°F). Where necessary, CNI cabinets are equipped with DC powered fans to ensure that maximum operating

temperature is not exceeded. To prevent air leaks, the units are provided with covers and are stacked with practically no clearance between them. The fan units are equipped with a filter that must be replaced on a routine basis to prevent clogging and reducing cooling performance.

3.1.3.2 Temperature, Humidity, and Altitude

Table 3.1-1 provides the operational temperature and humidity limits.

Table 3.1-1 Environmental Limits

PARAMETER DESCRIPTION	LIMITS
Operating temperature	+40°F to +100°F
Short-term temperature ^a	+35°F to +120°F
Wideband operating temperature ^b	+65°F to +80°F
Maximum rate of temperature change	15°F per hour
Operating relative humidity	20% to 55%
Short-term relative humidity ^c	20% to 80%
Notes: a. Short-term refers to a period of not more than 72 consecutive hours that the temperature should vary above or below the operating temperature and should not cover a period of more than 15 days in a year. b. Wideband operating temperature is the temperature range for the long-term operating periods. c. Relative humidity considerably less than 80% occurs for ambient temperature about 95°F. At short-term emergency condition of 120°F, the relative humidity should be below 20%.	

The CNI equipment is designed to operate when installed in offices located from 200 feet below sea level to 10,000 feet above sea level.

3.1.3.3 Electromagnetic Compatibility

The CNI equipment is designed for electromagnetic compatibility with existing central office equipment. The equipment continues to operate when the radio frequency fields are equal to or less than 10 volts per meter.

3.1.3.4 Electromagnetic Interference

The CNI equipment is designed to minimize electromagnetic interference. This equipment, like all telephone switching equipment, is temporarily exempt from Federal Communications Commission (FCC), Part 15, subpart J, regulations for class A computing devices.

3.1.3.5 Electrostatic Discharge

The CNI equipment is susceptible to electronic discharge and proper handling procedures must be observed.

3.2 RING TECHNOLOGIES

There are two different technologies used for CNI: Small Scale Integration (SSI) and Integrated Ring Node Version 2 (IRN2). The IRN2 is standard equipment. SSI was used for all installed rings up to and including software release 5E9(1).

NOTE: Effective January, 1997, SSI was rated Discontinued Availability (DA). New SSI hardware cannot be ordered.

3.2.1 SSI Ring

The SSI-based CNI ring uses two groups, 00 and 32, which are equipped identically for redundancy. Each group can be equipped with one RPCN, one DLN, and up to five LNs. The SSI CNI ring hardware can handle a maximum of 280,000 calls per hour.

NOTE: Effective January, 1997, SSI was rated Discontinued Availability (DA). New SSI hardware cannot be ordered.

3.2.2 IRN2 Ring

The IRN2-based CNI ring uses six groups: 00, 01, 02, 32, 33, and 34. These groups are split into two halves, one half consisting of groups 00, 01, and 02, the other half consisting of groups 32, 33, and 34. Each half of the ring is equipped identically for redundancy, and can be equipped with one RPCN, one DLN, and up to nineteen LNs. The IRN2 CNI ring hardware can handle up to 750,000 calls per hour, but is limited to 400,000 calls per hour by the 5ESS®-2000 switch hardware.

3.2.2.1 IRN2 Shelf Descriptions

There are two shelves used in the IRN2 configuration. One shelf (J3F011GD) contains positions for an RPCN, DLN, and three LNs, the other shelf (J3F011GC) contains positions for up to eight LNs.

3.2.2.2 IRN2 Node Components

Table 3.2-1 shows the packs that are required to make a particular node type. DLNs never use IFBs.

Table 3.2-1 IRN2 Components

Node Type	IRN2	LI	DDSBS	3BI	AP30
RPCN	X		X	X	
DLN30	X		X	X	X
LN	X	X			
IUN	X				

3.2.2.2.1 Integrated Ring Node Version 2 (IRN2)

The Integrated Ring Node Version 2 (IRN2) circuit pack (UN304B) combines the SSI-based NP, RI0, and RI1. It performs the NP functions using an *Intel*® 80386DX processor with 16 Mbytes of memory. The RI functions have been reduced to a VLSI chip.

3.2.2.2.2 Link Interface

The Link Interface circuit pack handles the transfer of information between the node processor and the signaling link. The link interface converts the signals from the node processor to a signal that is compatible with digital facility access frame circuits. The link interface circuit pack must be the TN916 (nonencrypted application) with the Processor Outage (PRO) feature (microcode MC3F030A).

3.2.2.2.3 Duplex Dual Serial Bus Selector (DDSBS)

The Duplex Dual Serial Bus Selector (DDSBS) circuit pack serves as a ring termination for the AM's dual serial channels (DSCHs). The DSCH provides high-speed buses for data transmission to and from the control units. The DSBS circuit pack is a TN69B.

3.2.2.2.4 3B20D/3B21D Computer Interface (3BI)

The TN914 circuit pack provides an interface between the RPCN node processor and the duplex dual serial bus selector. By controlling the direct memory access operation to each, the 3BI allows the node processor and the AM to send and receive when they are ready. The various control and status registers, along with the interrupt circuitry, allow the node processor (3BI and the duplex dual serial bus selector) to operate concurrently.

3.2.2.2.5 Attached Processor-30 (AP30)

The Attached Processor-30 (AP30) circuit (AP1630C) uses an MC68030 and 16Mbytes of memory to offload the CCS7 call processing from the AM. Messages are sent from the AP through the AM's DMA, via DDSBS and 3BI, to the Communications Module (CM).

3.2.2.2.6 Interframe Buffers

The ring interface circuits on the ring nodes drive each bus on the ring with a transistor-to-transistor logic type of signal and is limited to only a few inches of cable. Therefore, when the ring connection extends from the RPCN or LN on one ring node frame, to an RPCN or LN on the next ring node frame, the cable length restriction must be compensated. The interframe buffer provides balance drives and receivers that overcome the electrical problems of the longer cable. The interframe buffer circuit pack is TN1803.

3.2.2.3 IRN2 Cabinet Power Distribution

The power provided for the CNI meets the Underwriters Laboratories' requirements of a power plant of the single point ground type, in which all equipment is isolated from building ground. A negative 48-volt power supply is used to supply all load units in the CNI ring environment. Each cabinet power feeder powers one load unit. To minimize the number of nodes that could fail because of a single power converter failure, a single 410AA power converter is used to supply power to adjacent LNs and DLNs. Each RPCN is powered by a single converter.

See Figure 3.2-1 and Table 3.2-2 for the IRN2 ring cabinet power four node arrangement. See Figure 3.2-2 and Table 3.2-3 for the IRN2 ring cabinet power for more than four nodes.

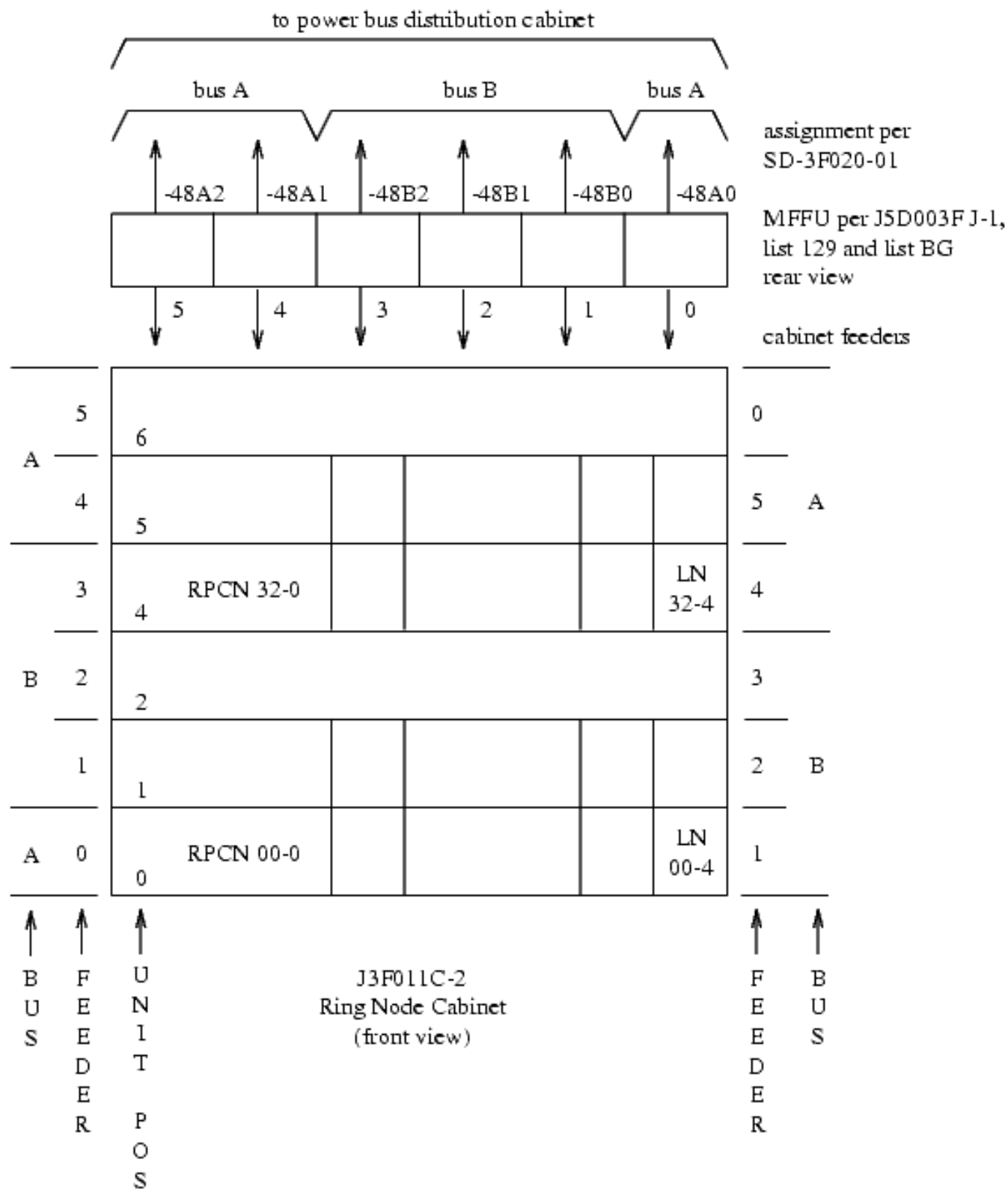
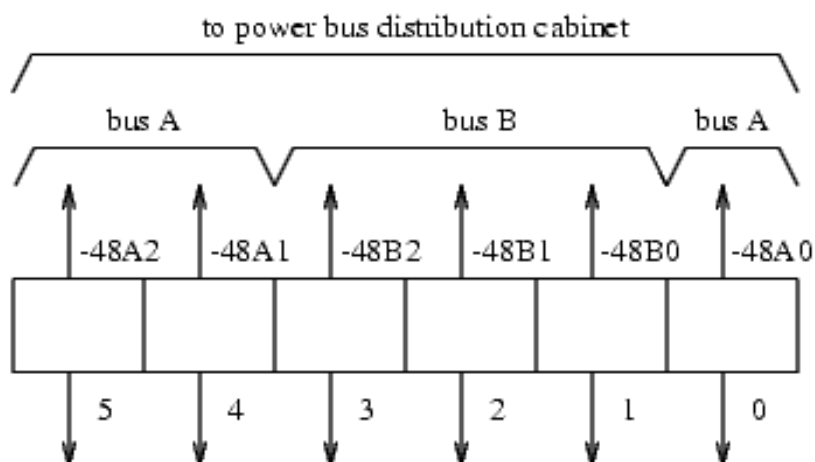


Figure 3.2-1 IRN2 Ring Cabinet Power - Four Node Arrangement

Table 3.2-2 IRN2 Ring Cabinet Power For Four Node Arrangement - Required Facility Assignment

Link Node J3F011C-2	DFA J3F010F-2
00-4	unit 0 slot 7
32-4	unit 0 slot 3



assignment per
SD-3F020-01

MFFU per J5D003F J-1,
list 129 and list BG
rear view

cabinet feeders

A2	5	6	LN 34-1	LN 34-2	LN 34-3	LN 34-4	LN 34-5	LN 34-6	LN 34-7	LN 34-8	0	A0
A1	4	5	LN 33-1	LN 33-2	LN 33-3	LN 33-4	LN 33-5	LN 33-6	LN 33-7	LN 33-8	5	A2
B2	3	4	RPCN 32-0		LN 32-1	DLN 32-2			LN 32-3	LN 32-4	4	A1
B1	2	2	LN 02-1	LN 02-2	LN 02-3	LN 02-4	LN 02-5	LN 02-6	LN 02-7	LN 02-8	3	B2
B0	1	1	LN 01-1	LN 01-2	LN 01-3	LN 01-4	LN 01-5	LN 01-6	LN 01-7	LN 01-8	2	B1
A0	0	0	RPCN 00-0		LN 00-1	DLN 00-2			LN 00-3	LN 00-4	1	B0

↑
B
U
S

↑
F
E
E
D
E
R

↑
U
N
I
T
P
O
S

J3F011C-2
Ring Node Cabinet
(front view)

↑
F
E
E
D
E
R

↑
B
U
S

Figure 3.2-2 IRN2 Ring Cabinet Power For More Than Four Nodes**Table 3.2-3 IRN2 Ring Cabinet Power For More Than Four Nodes - Required Facility Assignment**

Link Node	
J3F011C-2	J3F010F-2
00-1	unit 0 slot 1
00-3	unit 0 slot 6
00-4	unit 0 slot 7
01-7	unit 1 slot 5
01-8	unit 0 slot 8
32-1	unit 0 slot 5
32-3	unit 0 slot 2
32-4	unit 0 slot 3
33-7	unit 1 slot 1
33-8	unit 0 slot 4

3.2.2.4 IRN2 Frame Layout Rules

IRN2 rings have restricted configurations to allow ease of growth. Unlike the SSI-based rings, the number of LNs equipped determines the ring configuration. The following are the rules for the IRN2-based ring:

- (1) Only one CNI ring node cabinet is allowed per switch office.
- (2) RPCNs must be in groups 00 and 32 and only in position 0.
- (3) LNs can be in the following positions:
 - positions 1 through 8 in groups 01, 02, 33, and 34
 - positions 1, 3, and 4 in groups 00 and 32.
- (4) An IUN is only allowed in position 4 of groups 00 and 32.
- (5) LNs must be 56kbps non-encrypted.
- (6) DLN30 is only available when both positions 3 and 4 have been filled in groups 00 and 32.
- (7) DLN30s must be equipped if the call capacity of the office requires them. Refer to the 235-070-100, *Administration and Engineering Guidelines* for the maximum call capacity without DLNs.
- (8) Groups 00 and 32 must be filled before groups 01 and 33 can be equipped.
- (9) Groups 01 and 33 must be filled before groups 02 and 34 can be equipped.
- (10) All nodes must be grown from right to left on each shelf, except the RPCNs, which start on the left.

3.2.3 Backplane Attached Terminator (BAT) Board DSU/CSU Module

3.2.3.1 Introduction

3.2.3.1.1 General Description

The Lucent Technologies Backplane Attached Terminator (BAT) Board Data Service Unit/Channel Service Unit (DSU/CSU) Module, referred to hereafter as the DSU, is a single printed circuit board that performs the DSU/CSU functions for digital data service (DDS) networks. The DSU provides a 56K/64K synchronous interface to any dedicated DDS point-to-point network compatible with AT&T Publication 62310.

The latest digital signal processing and adaptive equalization techniques allow reliable extended loop operation (-45 dB) over non-loaded twisted pair cable. The DSU provides programmable options that give the customer flexibility to configure the device for different applications. The extensive use of VLSI technology provides high reliability and minimizes the size and power consumption of the DSU module.

Dual in-line package (DIP) switches provide the configuration and diagnostic control functions of the DSU. The DSU has an EIA 449 data terminal equipment (DTE) interface and an additional transisitor-transistor logic (TTL) DTE interface. Both interfaces are configured as data communications equipment (DCE). The DSU also provides an EIA 449 monitor port to allow checking of transmit and receive data with external equipment.

3.2.3.1.2 Front Panel

A diagram of the front panel is shown in Figure 3.2-3 .

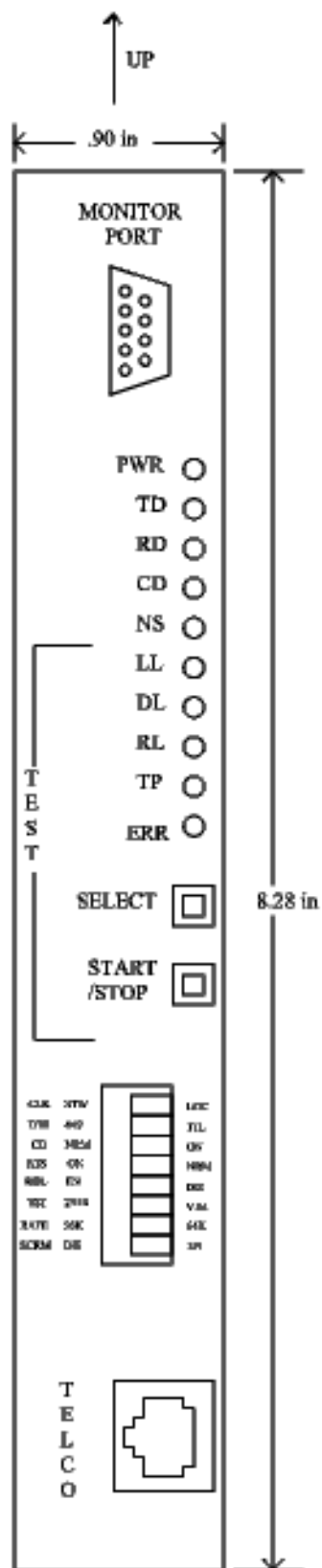


Figure 3.2-3 DSU Front Panel

The front panel of the DSU has an RJ48S network interface connector and an EIA 449 monitor connector. The front panel also has ten light-emitting diodes (LEDs) that indicate DTE interface, network, and test status. These indicators are:

Table 3.2-4 DSU Front Panel Indicators

DTE STATUS: (GREEN)	
LED	Function
PWR	ON - DSU is receiving power OFF - DSU is not receiving power
TD	ON - SPACE condition on the Transmit Data lead OFF - MARK condition on the Transmit Data lead
RD	ON - SPACE condition on the Receive Data lead OFF - MARK condition on the Receive Data lead
CD	ON - Carrier Detect is ACTIVE OFF - Carrier Detect is INACTIVE
NETWORK STATUS: (RED)	
LED	Function
NS	ON - Problem on the local loop or within the DDS network OFF - Normal loop and network conditions
TEST STATUS: (AMBER)	
LED	Function
LL	ON - A local loop (LL) test has been initiated from the front panel or the DTE interface. Data is being looped back to the DTE. FLASHING - A CSU loop interface test has been initiated by the service provider. Data is being looped back to the DTE.
DL	ON - A digital loop (DL) test has been initiated from the front panel. Data is being looped back to the network. FLASHING - A loop interface test (CSU or DSU loopback) has been initiated by the service provider. Data is being looped back to the network.
RL	ON - A remote digital loopback (RL) test has been initiated from the local DSU front panel or DTE interface (TTL only). FLASHING - A remote digital loopback test has been initiated from the remote DSU. Data is being looped back to the network.
TP	ON - The integral pattern generator is being used for testing.
TEST ERROR: (RED)	
LED	Function
ERR	FLASHING - Errors are detected during a test, or a test cannot initiate properly. The LED turns on for 1 second upon detection of each error.

The front panel also has two pushbutton switches that select and control the test modes of the DSU:

Table 3.2-5 DSU Front Panel Pushbutton Switches

Button	Description
TEST - SELECT	Press this button to select a test mode (indicated by one or more turned-on test status LEDs).
TEST - START/STOP	Press this button to initiate the selected test mode. Press this button to terminate a test that is in progress.

NOTE: Pressing the TEST-SELECT and TEST-START/STOP buttons simultaneously causes all LEDs to flash on and off at 1 second intervals. Continuing to depress both buttons for 5 seconds resets the DSU. Local tests initiate within 1 second. Remote tests initiate within 5 seconds.

3.2.3.2 Interface Signal Description

3.2.3.2.1 DTE Timing

The timing diagram for the EIA 449 interface is shown in Figure 3.2-4 .

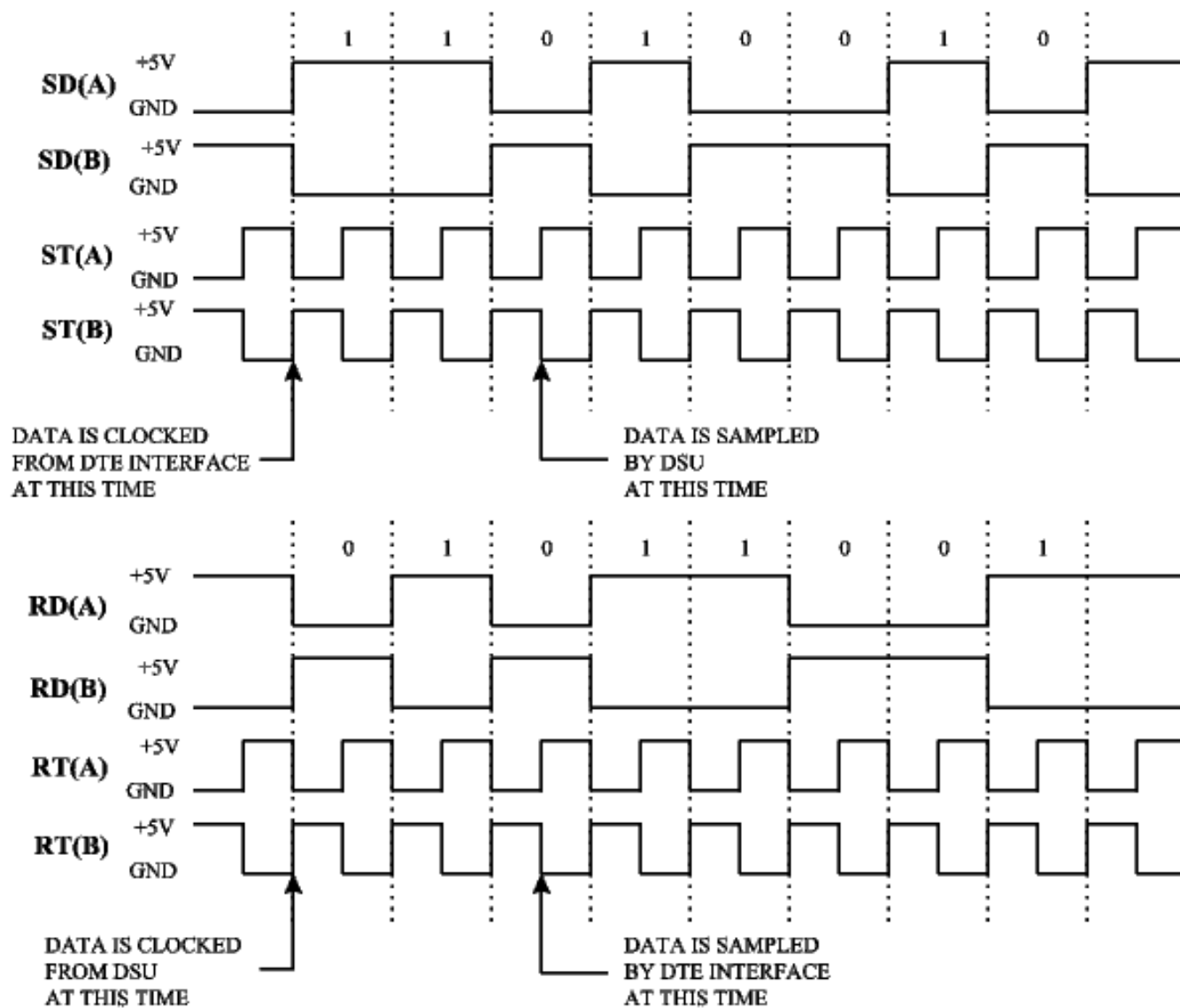


Figure 3.2-4 EIA 449 Data Interface Timing Diagram Backplane attached terminator EIA 449 Data Interface Timing Diagram BAT board EIA 449 Data Interface Timing Diagram

The timing diagram for the TTL interface is shown in Figure 3.2-5 .

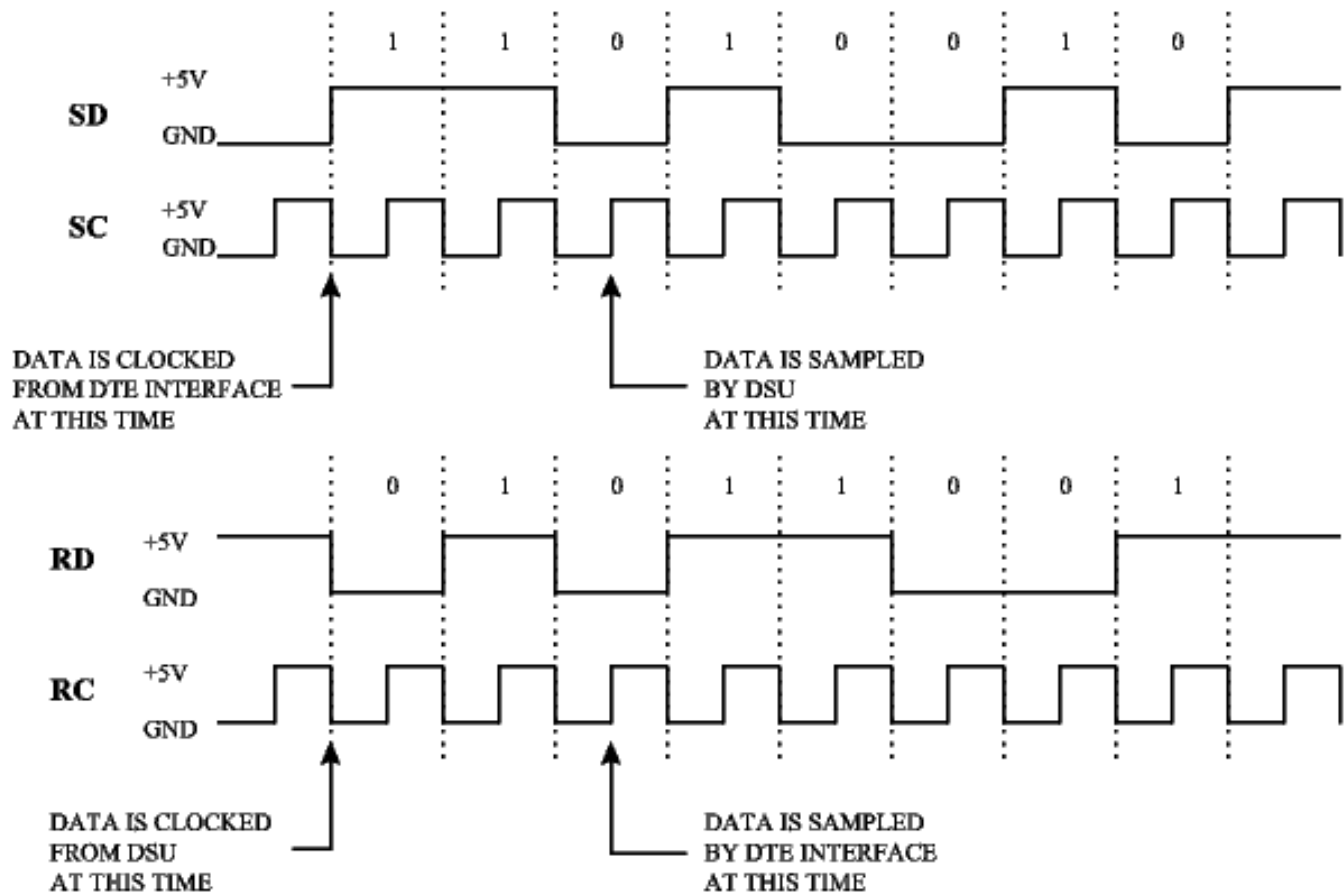


Figure 3.2-5 TTL Data Interface Timing Diagram Backplane attached terminator TTL Data Interface Timing Diagram BAT board TTL Data Interface Timing Diagram

The active state for the EIA 449 interface control signals is binary 0 (positive voltage). The active state for the TTL interface control signals is low (near 0 volts).

When connected to the LI4S (TTL) circuit pack, the DSU must be configured for TTL mode (switch 7). Since several of the port 1 signals on the LI4S conflict with the EIA 449 drivers on the DSU, provisions have been made to prevent damage to both the DSU and the LI4S. The LI4S (TTL) circuit pack presents +12 V on backplane pin 243, whereas the LI (449) circuit pack does not. Detection of the +12 V tri-states the EIA 449 drivers and receivers. A DTE interface mismatch causes all LEDs to flash fast (80 ms on/80 ms off) until the DSU is configured to match the backplane. When there is no DTE connected to the DSU (the DSU does not detect request to send [RTS]), the flashing is disabled to allow for loop testing.

3.2.3.2.2 Monitor Port Pin-Out

The monitor port consists of a female DB9 connector that provides transmit data, receive data, transmit clock, and receive clock via EIA 422 drivers. The monitor port is accessible from the front panel and provides the following EIA 449 leads:

Table 3.2-6 DB9 Monitor Port

Pin #	Signal	Description
1	SD (A)	Transmit Data (A)
2	SD (B)	Transmit Data (B)
3	SG	Signal Ground
4	RD (A)	Receive Data (A)

5	RD (B)	Receive Data (B)
6	ST (A)	Transmit Clock (A)
7	ST (B)	Transmit Clock (B)
8	RT (A)	Receive Clock (A)
9	RT (B)	Receive Clock (B)

3.2.3.2.3 Network Interface

The network interface consists of four leads that are paired to provide separate transmit and receive circuits. The four leads are provided on the eight-position modular jack RJ48S labeled TELCO on the front panel of the DSU.

Table 3.2-7 Network Interface

Symbol	RJ48S Pin #	Type	Name and Function Loop Interface
R1	1	O	Ring 1: Transmit data (to network interface)
T1	2	O	Tip 1: Transmit data (to network interface)
T	7	I	Tip: Receive data (from network interface)
R	8	I	Ring: Receive data (from network interface)

3.2.3.2.4 Hot Swap

The DSU is designed to be installed onto the powered-on backplane. The DSU limits inrush current with a network of inductors and capacitors (an L/C network), and uses interface integrated circuits that do not latch up when +5 V precedes the ground connection.

3.2.3.3 Configuration

The DSU has eight options for controlling the operation of both the network and DTE interfaces. These options are selected by setting individual switches on the eight-position DIP switch. Default configuration is shown in **BOLD**.

3.2.3.3.1 Switch 8 — Clock Source (Network/Local)

The Clock Source option specifies the timing source for the DSU's internal circuitry. When operating on a DDS network, the timing should be set to NTW. On a point-to-point private network, one DSU should be set for LOC, the other set for NTW.

Switch Position	Option
RIGHT	LOC
LEFT	NTW

3.2.3.3.2 Switch 7 — DTE Interface (EIA 449/TTL)

The DTE Interface option specifies which DTE interface to use. The LI circuit pack requires the DSU to be optioned for EIA 449 operation. The LI4S circuit pack requires the DSU to be optioned for TTL operation.

Switch Position	Option
RIGHT	TTL
LEFT	449

3.2.3.3.3 Switch 6 — Carrier Detect (CD) (Normal/On)

The Carrier Detect option allows the user to select one of two control modes for the CD lead. The NRM option configures the DSU to raise CD only when data is present on the loop. The ON option configures the DSU to hold the CD lead on at all times.

Switch Position	Option
RIGHT	ON
LEFT	NRM

3.2.3.3.4 Switch 5 — Request To Send (RTS) (On/Normal)

The Request To Send option defines how the DSU responds to RTS. In the NRM position, the DSU responds to RTS normally. In the ON position, the DSU ignores the state of RTS from the DTE and operates as if RTS is always on.

Switch Position	Option
RIGHT	NRM
LEFT	ON

3.2.3.3.5 Switch 4 — Remote Digital Loopback (RDL) (Enable/Disable)

The Remote Digital Loopback option determines how the DSU reacts to an RDL request. When set for EN, the DSU accepts a V.54 or 2556 DSU (configured with switch 3) compatible RDL command from the far end of the circuit. When set to DIS, the DSU ignores any RDL request from the far end.

Switch Position	Option
RIGHT	DIS
LEFT	EN

3.2.3.3.6 Switch 3 — Test Mode (TST) (2556/V.54)

The Test Mode option specifies the type of RDL command used and the test pattern generated by the internal test pattern generator. The 2556 option configures the DSU to be compatible with the 2556 DSU. The BAT board DSU generates and responds to 2556 loopback commands and uses a 511 test pattern. The V.54 option configures the DSU to be compatible with industry standard DSUs. The BAT board DSU generates and responds to industry standard V.54 loopback commands and uses a standard 2047 test pattern.

Switch Position	Option
RIGHT	V.54
LEFT	2556

3.2.3.3.7 Switch 2 — Loop Rate (56K/64K)

The Loop Rate option selects the DDS loop rate.

Switch Position	Option
RIGHT	64K
LEFT	56K

3.2.3.3.8 Switch 1 — Scrambler (Disable/Enable)

For 64K clear channel operation, there is a possibility that the DTE data sequences might mimic network loop maintenance functions and erroneously cause other network elements to activate loopbacks. To prevent this, set the SCRAMBLER option to EN. The scrambler must be enabled on both the local and remote DSUs for the situation described above (please clarify). This option is only valid when the 64K rate is selected. The scrambler should be disabled when transmitting data across a frame relay network.

Switch Position	Option
RIGHT	EN
LEFT	DIS

3.2.3.4 Test Modes

In addition to a self-test mode, the DSU has test modes that allow the user to isolate problems to specific components of the communications circuit. These tests are divided into two categories: tests initiated from the local DSU, and tests initiated remotely.

The local test can be initiated and terminated from the local DSU's front panel via the TEST-SELECT and TEST-START/STOP pushbuttons. Or, the test can be initiated from the DTE using the LL and RL (TTL only) leads. Front panel operation takes precedence over DTE operation.

The remote test can be initiated from either the remote DSU or the service provider.

3.2.3.4.1 Self-Test

When the DSU is powered on, all LEDs on the front panel turn on simultaneously for approximately two seconds. After two seconds, all the LEDs turn off briefly. The LEDs then cycle on in pairs with a fan-out pattern away from the NS LED. Next, the LEDs cycle off in pairs with a fan-in pattern toward the NS LED. These patterns are repeated four times so the user can determine that all LEDs are functioning properly.

At the completion of the LED test patterns, the TP LED is turned on to indicate that the LL WITH TP test is being performed. This test is successful when the ERR LED does not flash. If the LL WITH TP test fails, the NS, LL, and ERR LEDs all flash.

If a PROM CHECKSUM failure is detected during self-test, the PWR, CD, and NS LEDs all flash at the end of the self-test.

3.2.3.4.2 Locally-Initiated Test

The local DSU is capable of performing these locally-initiated tests:

- (1) Local Loop (LL)
- (2) Local Loop with Test Pattern (LL with TP)
- (3) Digital Loop (DL).

3.2.3.4.2.1 Local Loop (LL) Test

To initiate the LL test, press the TEST-SELECT button once to turn on the LL test LED, then press the TEST-START/STOP button while the LL test LED is on. The LL LED flashes during initialization of the test.

The LL test provides a method for testing both the DTE interface of the local DSU plus its loop transmitter and receiver. For this test, the loop transmit data is connected to the loop receive data at a point close to the physical network interface. The DSU transmits all zeroes to the network during this test. During normal operation of this test, the LL LED remains on without flashing. A block diagram illustrating the loopback point and the signal paths for this test is shown in Figure 3.2-6.

Test data from the terminal or test equipment is routed through the DTE section of the DSU and then to the output of the loop transmitter section, where the signal is encoded for transmission. The output of the loop transmitter is coupled back to the loop receiver input. This receive test signal is then decoded and returned to the terminal or test equipment where it is checked for bit errors.

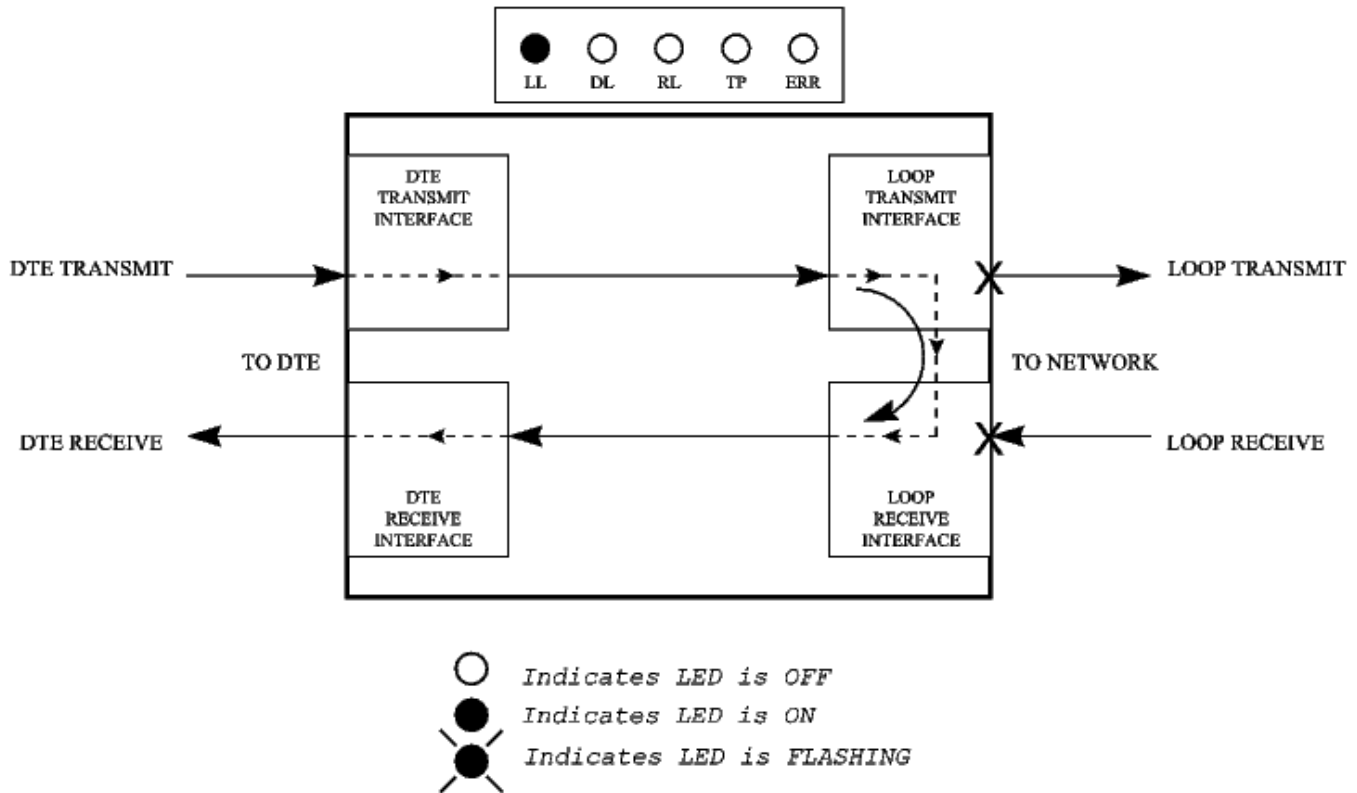


Figure 3.2-6 LL Test

3.2.3.4.2.2 LL with TP (Test Pattern)

To initiate the LL WITH TP test, press the TEST-SELECT button twice to turn on the LL and TP test indicators, then press the TEST-START/STOP button while the LL and TP test indicators are on. The LL and TP LEDs flash during initialization of the test. The ERR LED is turned on for 1 second during initialization of the test.

The LL WITH TP (test pattern) test is similar to the LL test described in section 3.2.3.4.2.1. It is initiated at the local DSU and is used to independently test the operation of the DSU.

Instead of using data from the terminal or test equipment, the LL WITH TP test uses an internal test pattern generator and detector built into the DSU. The loopback point and the data paths for this test are illustrated in Figure 3.2-7.

The internal test pattern generator and detector of the DSU operate with a 511 or 2047 (switch 3) data pattern. When the LL WITH TP test is initiated, the test pattern detector examines the receive data stream until synchronization to the test pattern is achieved. When synchronized, the detector continues to check the receive data and reports bit errors by flashing the ERR LED.

When a test is initiated with the internal test pattern generator and detector, errors can be injected into the transmit data stream by pressing the TEST-SELECT button and observed when the ERR LED illuminates.

As previously mentioned, the LL WITH TP is automatically performed during the self-test sequence for the DSU.

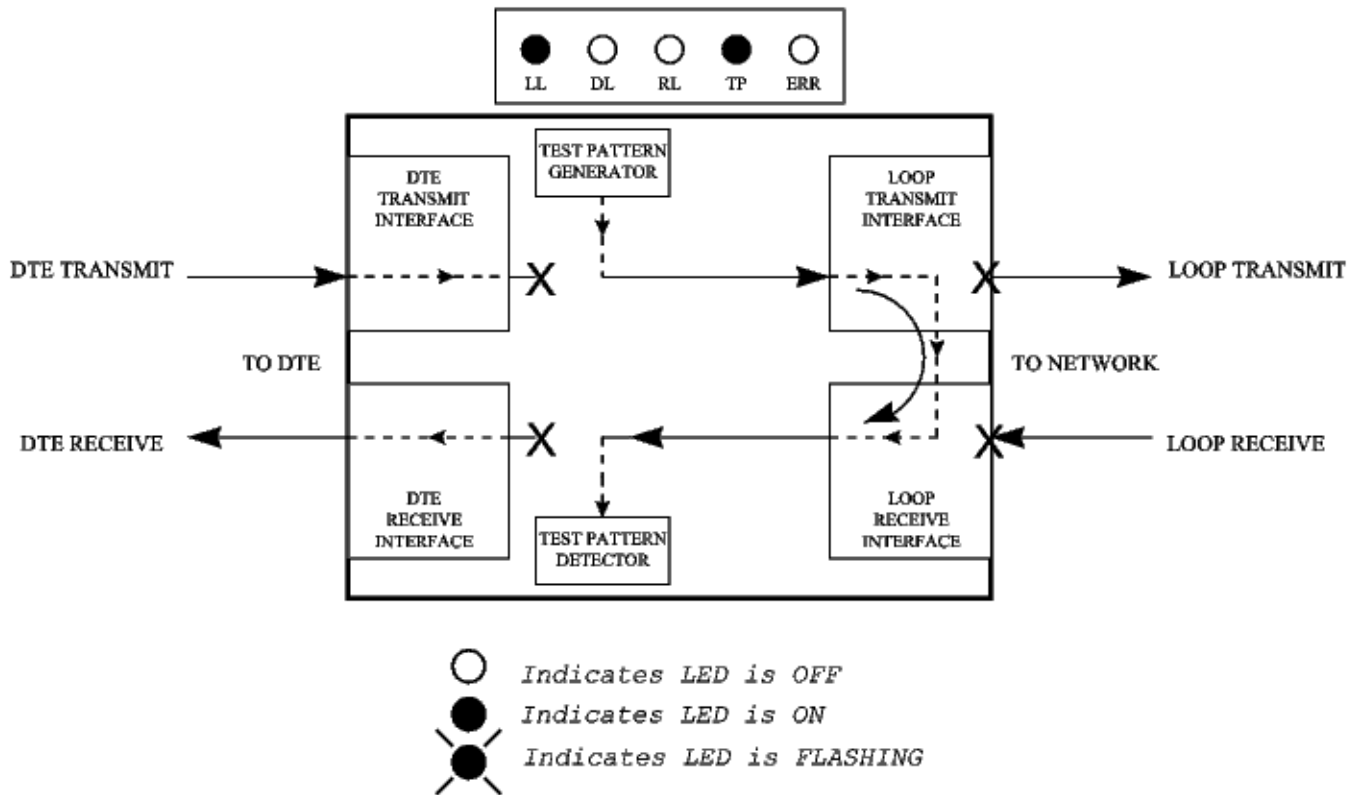


Figure 3.2-7 LL with TP Test

3.2.3.4.2.3 Digital Loop (DL) Test

To initiate the DL test, press the TEST-SELECT button three times to turn on the DL test LED, then press the TEST-START/STOP button while the DL test LED is on. The DL LED flashes during initialization of the test and turns on without flashing when the test is in progress.

The DL test allows the loop interface and a major portion of the DTE interface of the local DSU to be tested from the remote site over the actual DDS circuit.

For the DL test, the network receive data is looped to the network transmit data inside the DTE interface section of the DSU. The physical DTE interface is ignored for the DL test. A block diagram illustrating the loopback point and the signal paths for this test is shown in Figure 3.2-8.

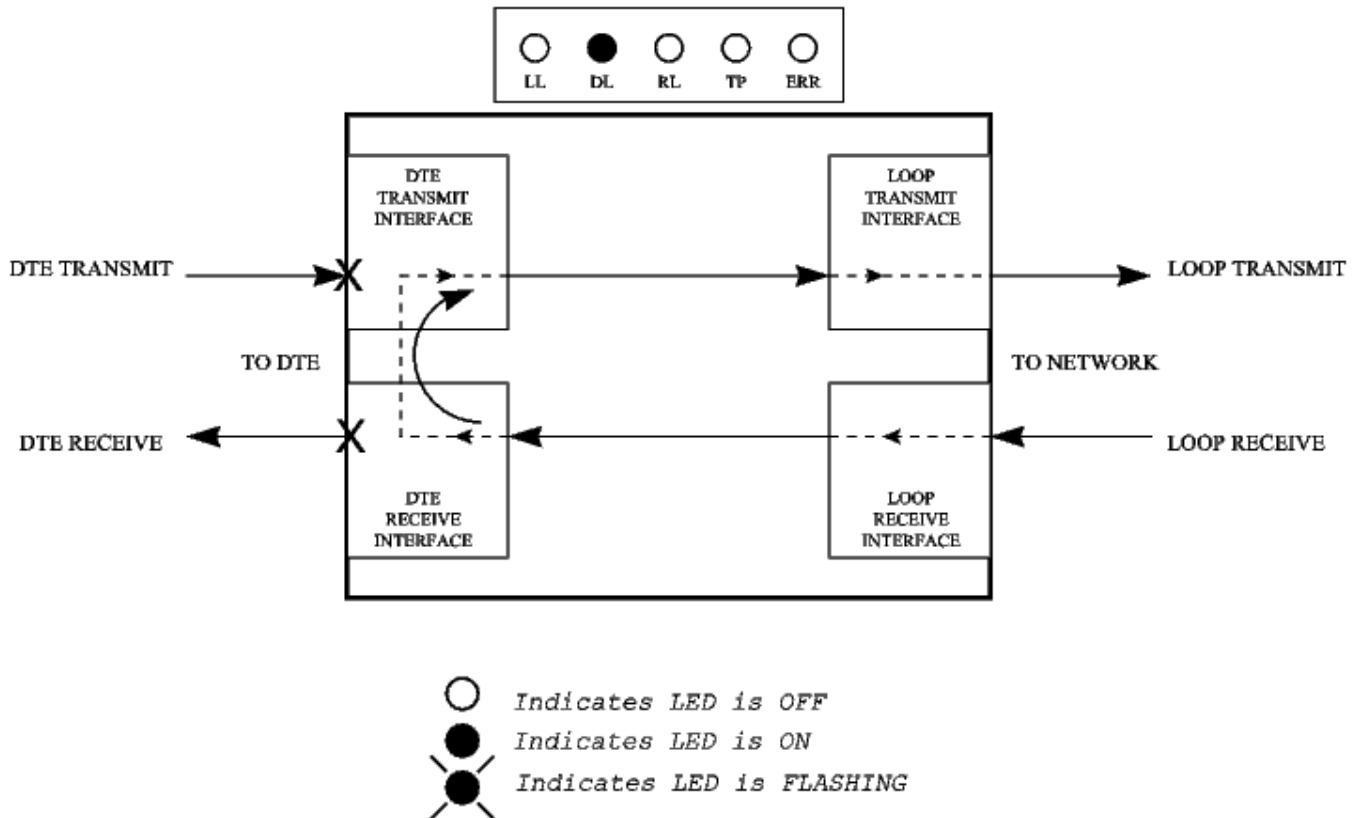


Figure 3.2-8 DL Test

3.2.3.4.2.4 Remote Digital Loopback (RL) Test

To initiate the RL test, press the TEST-SELECT button four times to turn on the RL test LED, then press the TEST-START/STOP button while the RL test LED is on. The RL LED flashes during initialization of the test and turns on without flashing when the test is in progress. The ERR LED illuminates and remains on without flashing until the remote loop is established.

When the RL test is initiated at the local DSU, it commands the remote DSU into loopback with an 2556 DSU or V.54 (selected by SW 3) compatible loopback pattern. The loopback point and the signal paths for the remote DSU are the same as the DL test for a local DSU, see Figure 3.2-9. This loopback test is performed with data from the DTE or test equipment.

NOTE: In V.54 mode, if the remote loopback cannot be established within approximately 4 seconds, the remote loopback request is dropped automatically.

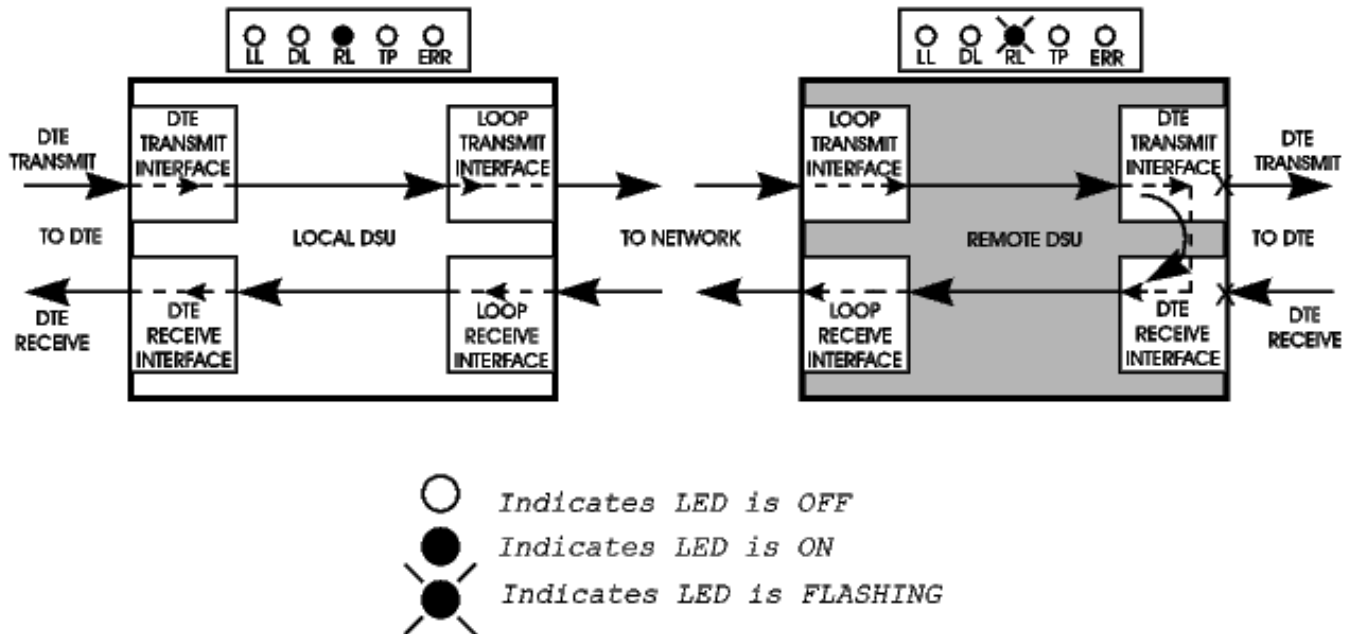


Figure 3.2-9 RL Test

3.2.3.4.2.5 RL with TP

To initiate the RL WITH TP test, press the TEST-SELECT button five times to turn on the RL and TP test LEDs, then press the TEST-START/STOP button while the RL and TP test LEDs are on. The RL and TP LEDs flash during initialization of the test and turn on without flashing when the test is in progress. The ERR LED illuminates and remains on without flashing until the remote loopback is established.

When the RL WITH TP test is initiated at the local DSU, it commands the remote DSU into loopback with a 2556 DSU or V.54 (selected by switch 3) compatible loopback pattern. The loopback point and the signal paths for the remote DSU are the same as the DL test for a local DSU, see Figure 3.2-10. The RL WITH TP test uses the internal test pattern generator and error detector. When synchronized, the detector continues to check the receive data, and reports bit errors by flashing the ERR LED.

NOTE: In V.54 mode, if the remote loopback cannot be established within approximately 4 seconds, the remote loopback request is dropped automatically.

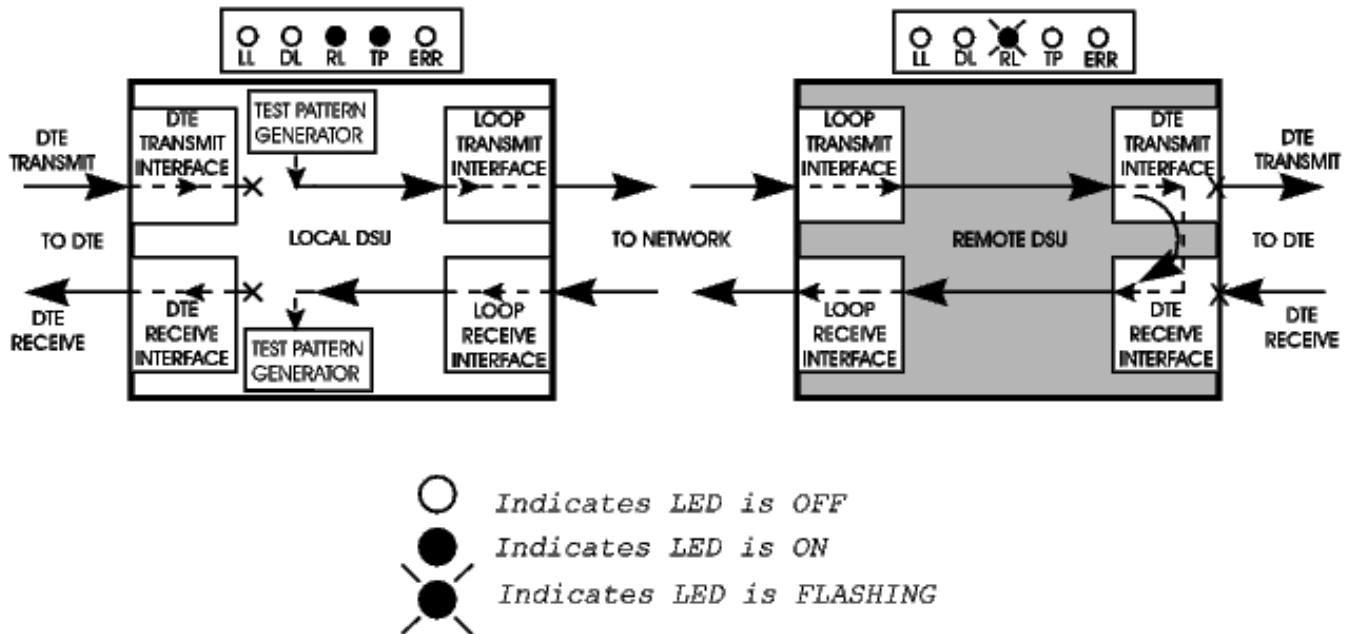


Figure 3.2-10 RL with TP Test

3.2.3.4.2.6 Test Pattern (TP)

To initiate the TP test, press the TEST-SELECT button six times to turn on the TP test indicator, then press the TEST-START/STOP button while the TP test indicator is on. The TP LED flashes during initialization of the test and turns on without flashing when the test is in progress. The ERR LED is illuminated during initialization of the test.

When the TP test is initiated, the local DSU uses the integral test pattern generator to transmit a standard 511 or 2047 (switch 3) test pattern to the DSU at the far end of the circuit, see Figure 3.2-11. The local DSU then examines the receive data for the standard test pattern. The ERR indicator flashes when errors in the receive data pattern are detected. While the TP test is active, errors can be injected into the transmit data stream by pressing the TEST-SELECT button.

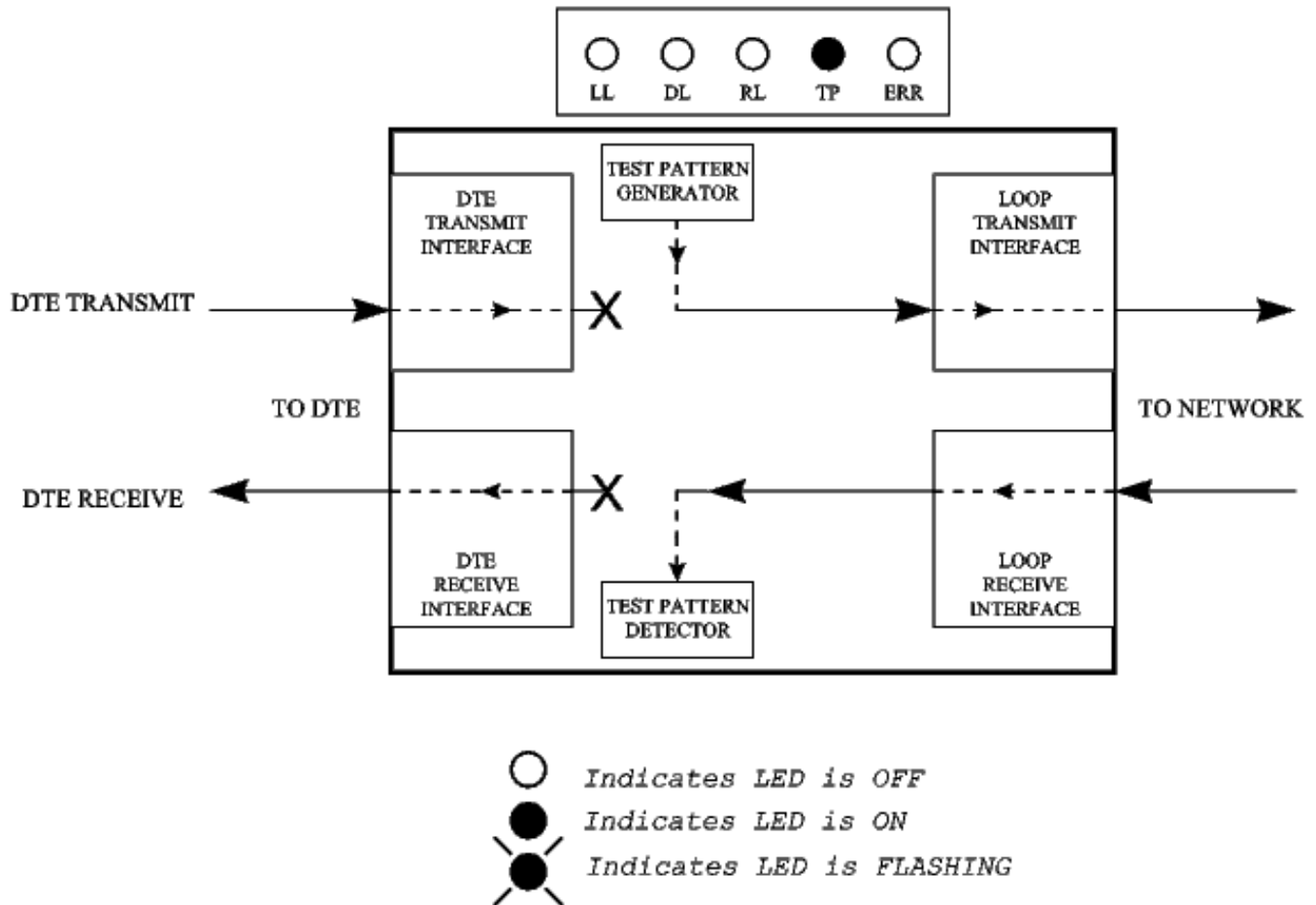


Figure 3.2-11 TP Test

3.2.3.4.3 Remotely-Activated Tests

The DSU responds to these three remotely-activated tests:

- (1) Remote Digital Loopback (RL)
- (2) CSU Loopback
- (3) DSU Loopback.

3.2.3.4.3.1 Remote Digital Loopback

The RL test is initiated by a remote DSU and causes the local DSU to loop back. The loopback point is the same as the DL point shown in Figure 3.2-12. The RL test checks the end-to-end performance of the circuit. The local unit flashes the RL LED.

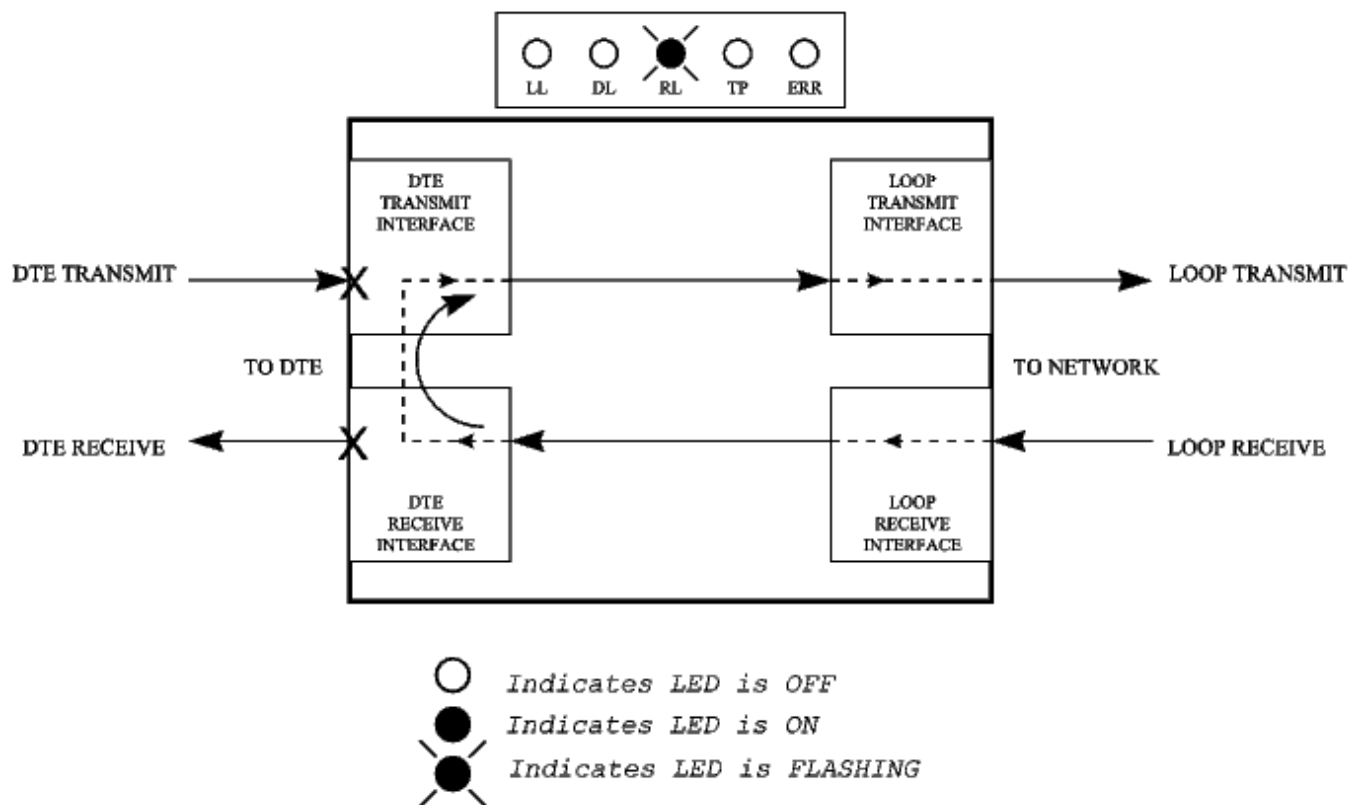


Figure 3.2-12 Remote Digital Loopback

3.2.3.4.3.2 CSU Loopback

The CSU LOOPBACK test is activated from the service provider's diagnostic test equipment by reversing the loop sealing current, and is used to isolate trouble on a circuit. The CSU portion of the unit is looped toward the network, see Figure 3.2-13. The local unit flashes the DL LED (80 ms on, 80 ms off).

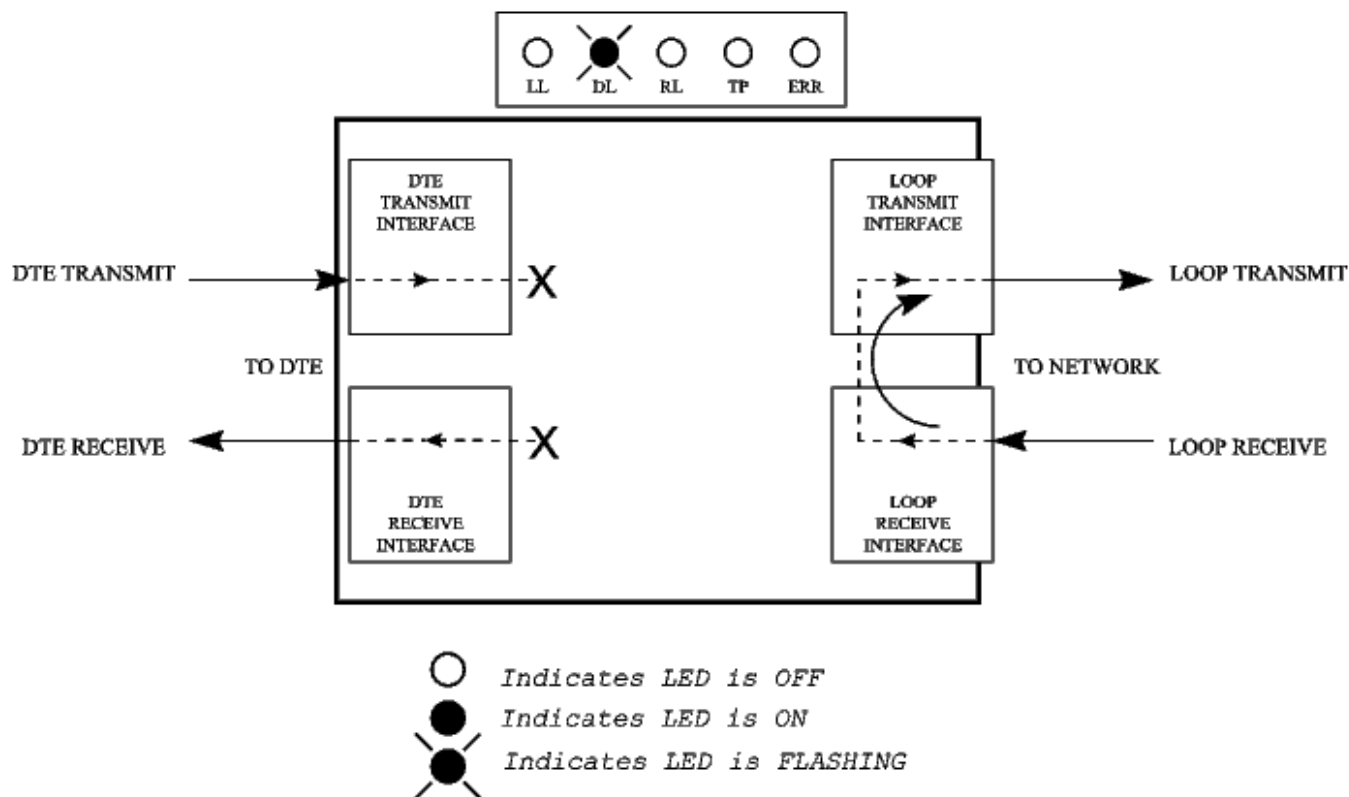


Figure 3.2-13 CSU Loopback

3.2.3.4.3.3 DSU Loopback

The DSU LOOPBACK test is activated from the service provider's diagnostic test equipment, and is used to isolate trouble on a circuit. The DSU portion of the unit is looped toward the network, see Figure 3.2-14 . The local unit flashes the DL LED (480 ms on, 480 ms off).

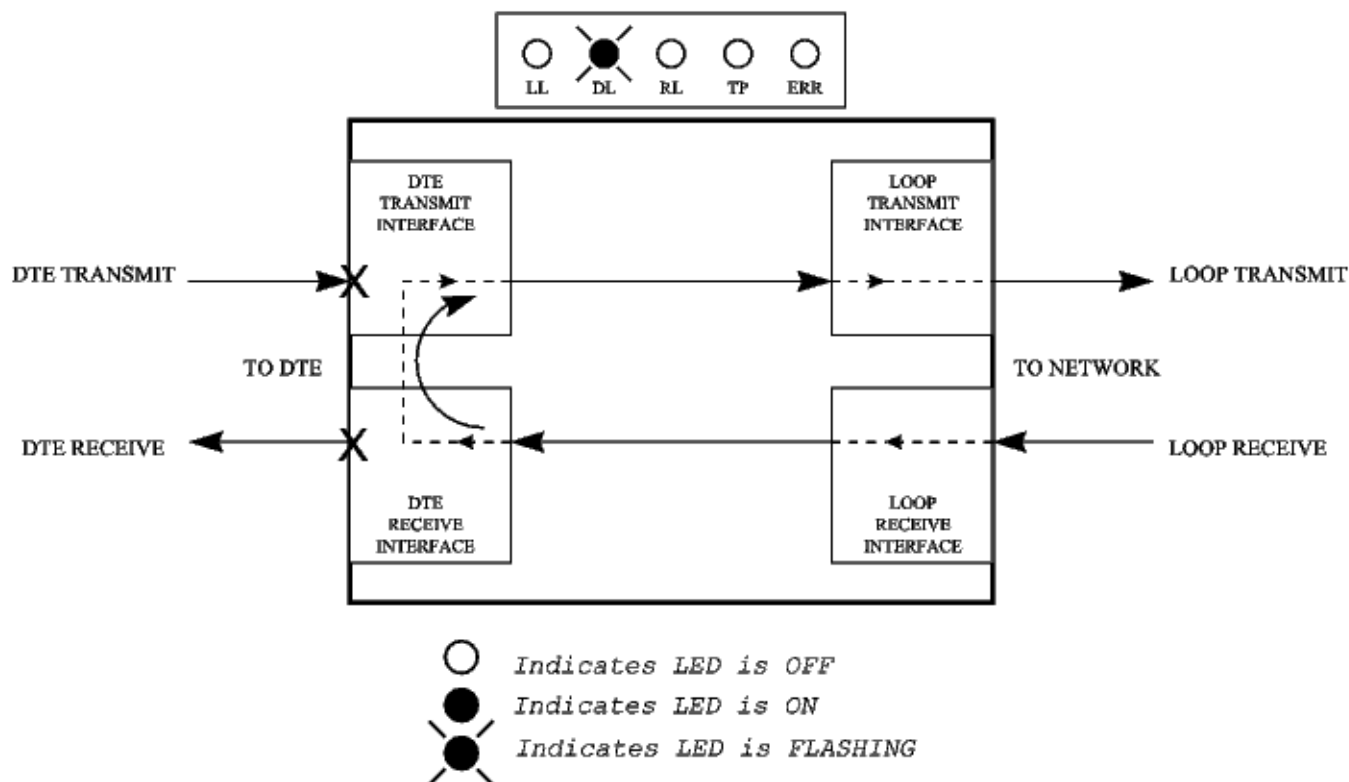


Figure 3.2-14 DSU Loopback

3.2.3.5 Compliance Requirements

The BAT board DSU is designed to meet these specifications:

FCC Part 68

FCC Part 15 Class A

Network Equipment Building Systems (NEBS)

Bellcore 1089 (Power Cross and Lightning sections only)

3.2.3.6 Specifications Summary

The standard specifications and features incorporated in the DSU are:

Loop Interface:	4-wire, full duplex
Line Requirements:	Local loop specifications per AT&T Publication 62310
Receiver Sensitivity:	- 45 dB
DTE Interfaces:	EIA 449 and TTL synchronous
DTE Operating Modes:	Full or half duplex
Data Rates:	56K or 64K synchronous

Diagnostics:

- (1) Network test center activated:
 - (a) CSU loopback on sealing current reversal
 - (b) DSU loopback

- (2) User activated:
 - (a) Self test
 - (b) Local loopback
 - (c) 2556 compatible remotely-activated loopback with:
 - (i) 511 test pattern
 - (ii) DTE data
 - OR —
 - (d) V.54 compatible remotely-activated loopback with:
 - (i) 2047 test pattern
 - (ii) DTE data

Environment:

- (1) Temperature —
 - Operating: 0° to 57°C (32° to 135°F)
 - Storage: -20° to 70°C (-4° to 158°F)
- (2) Relative humidity — up to 95% noncondensing

3.3 SYSTEM OPERATION AND ADMINISTRATION

3.3.1 CNI System Operation

3.3.1.1 Interprocessing Message Switch (IMS)

The core of CNI is the IMS, which is a high capacity packet switch. The IMS system routes data messages between the switch call processing software by using a direct memory access (DMA) channel to the ring peripheral processors with a minimal amount of delay. The IMS also transports messages between nodes on the ring. To support communications and maintenance of the CNI hardware, the AM operating system provides user interface terminals, printers, disk storage, and software.

The CNI/IMS uses the switch AM computer as the central processing unit. This unit runs on a *UNIX*[®] real-time reliable operating system, which must have a minimum of 30 mb memory when CNI is equipped. The AM processor interfaces with the ring processor control nodes by using a DSCH. Nodes on the CNI ring communicate with each other by using a ring type local network. The link nodes are points where signaling information leaves or enters the switch.

The CNI peripheral processing elements are the RPCNs, LNs, DLNs, and IUNs. All of these contain ring interface and node processor circuitry.

The functions of the RPCNs, LNs, DLNs, and IUNs are as follows:

- The RPCNs provide communications between the ring and AM.
- The DLN processors are used to perform signaling message processing normally performed by the switch AM when DLNs are not present. This relieves the AM of some real-time functions to provide more CCS call processing capacity. The DLNs are interconnected to the other nodes on the ring by the dual ring bus, and to the AM by using the DSCH for call processing similar to the RPCNs. The DLN/CM connection is accomplished through reading and writing of shared memory in the AM. This does not use any AM real time for DLN/CM communication.
- The LNs provide communications between the ring and CCS network. The LN data speeds can be 4.8 kb/s or 56 kb/s. Both protocols can be either encrypted or nonencrypted.
- The IUN is an equipped node on the ring, but can do no signaling or processing. To avoid ring cabling at time of LN growth, the IUN may be used in the switch CNI ring to build future LNs.

All nodes are interconnected by a dual ring bus which provides access between the nodes for internode communication. The local network uses an internal packet communication protocol independent from any application network protocols.

3.3.1.2 CNI Related Software

All of the IMS, CNI, and CCS software have been integrated into the switch software release. The software components include the following:

- ***The 3BRTR computer operating system***
- ***The CNI software*** - The interprocess message switch (IMS) and the CNI interface components (including the RPCN and DLN software components)
- ***The switch software*** - The recent change, initialization, system integrity, and call processing.

The AM operating system is the real-time reliable (RTR) operating system. The software contains features necessary to meet the demands of real-time switching and telecommunications systems. The system procedures allow the CNI to efficiently share the computer and resources (that is, computer time, storage space, and peripheral devices). The time critical code for message switching coexists with time-shared software as background tasks.

The CNI software system allows multiprocessing of nodes in a reliable environment. Message transport is in a packet message format. The processing is based on a ring node interconnect structure. The system contains the software for interprocess communication, personnel interface, hardware maintenance, system initialization, audits, and measurements. Also included is the message-distributing software in the central processor. This system's software uses an internal communications protocol and is independent of all signaling network protocols.

The breakdown of the functions performed through the use of the software components is shown in Table 3.3-1. The node process functions are shown in Table 3.3-2.

Table 3.3-1 Administrative Module Functions

SOFTWARE	FUNCTIONS
UNIX [®] SYSTEM RTR	• User program documentation standards command execution and display page access • Audit control • Execution environment for all CNI 3B resident software • Equipment configuration data maintenance.
CNI/IMS	• Initialization • Measurement and critical event generation • Measurement data cumulation, history file maintenance, and report generation • CCIS network critical event log file maintenance and message distributing • SS7 signaling load balancing • Data base updating (point code routing data, link data, and measurement output control table data) • Link management and link status auditing • Overload and insanity detection • Error detection, error message analysis, and ring recovery • Maintenance of ring and nodes, and ring reconfiguration • Diagnostics administration • Real-time overload control and insanity detection • Ring node control auditing • Software trace reporting control

	• Message switching.
5ESS [®] -2000 Switch	• Measurement generation • System initialization • Translation of CCS routing labels to SM/port (non-DLN configuration) • Network management for direct signaling (non-DLN configuration) • Recent change and verify • CCS call processing (non-DLN configuration) • Display Page 118 updates • Event trapping • Routing of TCAP messages (non-DLN configuration) • Adding OSDS header to trunk signaling messages (non-DLN configuration) • I/O messages • Ring Silence Monitoring.

Table 3.3-2 Node Processor Functions

NODE TYPE	FUNCTIONS
RPCN	• Measurement generation • Error detection • Ring hardware state data administration • Maintenance and stand-alone ring and node processor diagnostics • Message flow control to central processor • Local audit control (for example, neighbor node audits)
LN	• Transporting signal messages and interprocess messages between ring and central processor • Measurement generation • Link interface diagnostics • Overload and congestion controls • Discrimination and distribution of messages from the ring to network

	• Alternate routing for banded messages • Link and signaling route management • Signaling link protocol execution.
DLN (From CNI/IMS)	• Measurement generation • Ring hardware state data administration • Maintenance and stand-alone ring and node processor diagnostics • Translation of CCS routing labels to SM/port for trunk signaling • Routing of TCAP messages.
(From 5ESS®-2000 Switch)	• Network management control for direct signaling • Event trapping for direct signaling • Adding OSDS headers to trunk signaling messages.

The switch software includes a portion of the AM-resident software, a portion of the node processor resident software, initialization, recent change, and call processing software.

3.3.2 Independent Ring Access Circuits And Data Selectors

3.3.2.1 Purpose of Ring Access Circuit and Data Selector

Each ring interface consists of a pair of independent ring access circuits and data selectors. The ring access circuit allows messages to be inserted onto, removed from, or passed along a specific ring. The node processor communicates with each of its ring access circuits by using direct memory access buses. Then, the data selectors redirect the data from one part of the ring to another.

The ring access circuit examines the message to determine its destination. If the message is destined for the node, of which the ring access circuit is a part, the direct memory access controller reads the message into the dual part memory. If the message is not destined for that particular node, it is passed on to the next node in the ring.

3.3.2.2 Token Message

A special message called the *token message* travels around each ring, and allows other messages to be placed on the ring without causing congestion. When a node has a message to send to the ring, the ring access circuit of the *upstream* node detects and holds the token message, until the node with the message transmits it to the ring, then releases the token message. Data is passed from one ring access circuit to the next in a synchronous fashion. Messages can be written in blocks containing either a single message or multiple messages. These message packets are delivered to their destination node using the physical address and the address specified in the message. In addition to the destination address, a destination "channel" is also specified in the message to identify the software function that receives the message.

3.3.2.3 Reading a Packet from the Ring

The normal sequence for reading from the ring is as follows:

- (1) The ring access circuit detects its node address in the message and starts the direct memory access.
- (2) The direct memory access controller sends the message to the node processor buffer.
- (3) The message is queued for the user of the destination channel. If there are multiple messages back-to-back on the ring that are all destined for the same node, they are directed by the direct memory access into the node processor memory before the messages are distributed to their destination channels.

3.3.2.4 Writing a Packet to the Ring

Message packets are written to the ring as follows:

- (1) Messages are queued in the node processor buffer until the token is detected by the ring access circuit at the upstream node.
- (2) While the token message is held by the ring access circuit of node "n," the direct memory access sends all waiting messages of node "n+1" to the ring.
- (3) If the size of the total waiting message exceeds the maximum size of one message, the message is broken into blocks no larger than the maximum message size. It may take multiple token message visits to complete the writing of all waiting messages to the ring.

3.3.3 Token Tracking

There may be conditions in the CNI ring that cause the unexplained loss of the token message. To save time in finding the lost token on the CNI/IMS ring, token tracking is available. Although unexplained token loss is not common in the switch, there have been some reports of this problem.

The hardware incorporates token-tracking flip-flops that toggle whenever a token visits a node. The token-tracking software is executed whenever an unexplained loss of token occurs. The interprocess message switch software module interrogates the ring, collecting data available from the token-tracking flip-flops. The data is analyzed by the software and from the bit pattern, also identifies the vicinity of the loss-of-token. A message on the read-only printer indicates the range of nodes on the ring where the loss-of-token has occurred. The token-tracking software does not take any recovery action, but simply identifies the vicinity of the loss-of-token. Token loss can be due to software and/or hardware problems.

The token-tracking software can cause the token to be lost when a ring segment is isolated and a fault occurs. Such cases are sporadic and cannot be corrected by the office personnel; however, they can be minimized if the whole ring is normally kept active (no isolated nodes).

If token loss occurs frequently on the same node, while the whole ring was active, it is probably a hardware problem. The suspect node should have the bad boards replaced. Typically, the bad boards are ring interface (RI0 and RI1), but node processor (NP) and interframe/intraframe buffers (IFB) can cause this problem too.

With or without token tracking, the CNI ring should recover automatically after the RPCN detects the token loss; however, the potential problem still exists until the source of the problem is eliminated.

Without token tracking, if the loss of token occurs frequently, the solution is to isolate nodes one at a time until a configuration is found in which the node that is losing the token is not in the active ring. IRN2 rings have token tracking built in.

3.3.4 Equipment Configuration Data Base

3.3.4.1 Unit Control Block

The definition of the CNI ring nodes that are equipped and the placement of the buffer packs is contained in the Unit Control Block (UCB) forms in the equipment configuration data base. Table 3.3-3 aids in populating the UCB forms for the IRN2 CNI ring nodes. The fields shown are critical in equipping the ring and ring configuration.

There are UCB forms required for the RPCN and DLN Dual Serial Channels, when an RPCN or DLN is equipped. With each DLN, an RPCD form is also required.

Table 3.3-3 IRN2 CNI Node UCB Population Aid

FIELD NO.	FIELD NAME	NODE TYPE ^a					
		RPCN		LN	DLN		
3	unit_name:	RPCN00	RPCN32	LNww	LNww	RPCD00	RPCD32
4	unit_number:	0	0	x	2	2	2
13	internal_device	no entry	1	no entry	no entry	2	3
23	device_num	2 1 b	3 1 b	null	null	4 2 b	5 2 b
25	hv:	y	y	y	y	y	y
27	mv:	0x2	0x2	0x43	0x23	0x23	0x23
28	interrupt_num	2 1 b	3 1 b	no entry no entry	no entry no entry	4 2 b	5 2 b
30	pathname	pu/rpc	pu/rpc	pu/irn2	pu/irn2	pu/ DLNI_ NA	pu/ DLNI_ NA
62	packcode	RPC	RPC	C7I2	DL23	DL23	DL23
63	issue	1	1	1	1	1	1
Notes: a. Where: ww = group number (00, 01, 02, 32, 33, or 34) x = node member number (1, 3, 4, 5, 6, 7, 8) y = Hardware Version (HV) b. These values are for 3B21D only.							

Field 25, hardware version (HV) value, is critical for ring configurations. The HV value defines the position and type of buffer packs in the ring relative to the node. Using the data flow as reference, a node may have an adjacent buffer pack either upstream, downstream, or no buffer at all. Table 3.3-4 provides the IRN2 HV values. The 0x1XX values are changed to 0x19XX (for example, the RPCN HV values are changed from 0x102 to 0x1902) for token-tracking hardware.

Table 3.3-4 IRN2 UCB Field 25 Hardware Version (HV) Values

GROUP	RPCN	LN-1	DLN/LN-2	LN-3	LN-4	LN-5,6,7	LN-8
00	0xc006	0xc000	0x200c000	0xc000	X ^a	NA ^b	NA ^b
01	NA ^b	0xc000	0xc000	0xc000	0xc000	0xc000	Y ^c
02	NA ^b	0xc000	0xc000	0xc000	0xc000	0xc000	0xc000
32	0xc006	0xc000	0x200c000	0xc000	X ^a	NA ^b	NA ^b
33	NA ^b	0xc000	0xc000	0xc000	0xc000	0xc000	Y ^c
34	NA ^b	0xc000	0xc000	0xc000	0xc000	0xc000	0xc000
Notes: a. X = If LN01-08 and LN33-38 are equipped, use 0xc000. Otherwise, set to 0xc060. b. NA = Not Applicable. c. Y = Yes.							

b. NA = Not applicable.

c. Y = If LN02-08 and LN34-38 are equipped, use 0xc000. Otherwise, set to 0xc060.

3.3.4.2 Verifying Pointers in Required Unit Control Block (UCB) Forms (3B20D)

The pointers in each of the UCB forms should be checked. If the CNI is equipped with a DLN, it is important to verify that the pointers on all related UCB forms include the DLN.

Referring to Figure 3.3-1, check forms RPCN32 0, RPCD00 2, and RPCD32 2 to verify that the proper pointers exist.

(1) To verify the pointers for RPCN32:

- At Fields 1 and 2, hit the carriage return.
- At Field 3, (k_unit_name), enter **RPCN32**.
- At Field 4, (K_unit_number), enter **0**.
- The rest of the form is filled in.
- Go to Page 3 of the form.
- There must be a side pointer to the DLN:
 - Field 44 must be **RPCD00**
 - Field 45 must be **2**.
- If these fields are not correct, make these changes and exit the form.

(2) To verify the pointers for RPCD00:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **RPCD00**.
- At Field 4, (k_unit_number), enter **2**.
- The rest of the form is filled in.
- Go to Page 3 of the form
- There must be a side pointer to the other DLN.
 - Field 44 must be **RPCD32**
 - Field 45 must be **2**.
- The control pointers must exist as follows:

FIELD	ENTRY	FIELD	ENTRY
46	cntrl_0	47	CU
48	0	49	CH

50	12	51	cntrl_1
52	CU	53	1
54	CH	55	12

- If these fields are not correct, make the changes and exit the form.

(3) To verify the pointers for RPCD32:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **RPCD32**.
- At Field 4, (k_unit_number), enter **2**.
- Response: The rest of the form is filled in.
- Go to Page 3 of the form.
- There are no pointers, Fields 44 and 45 are blank.
- Control pointers (46 through 55) are the same as for RPCD00 2.
- If these fields are not correct, make these changes, then exit the form.

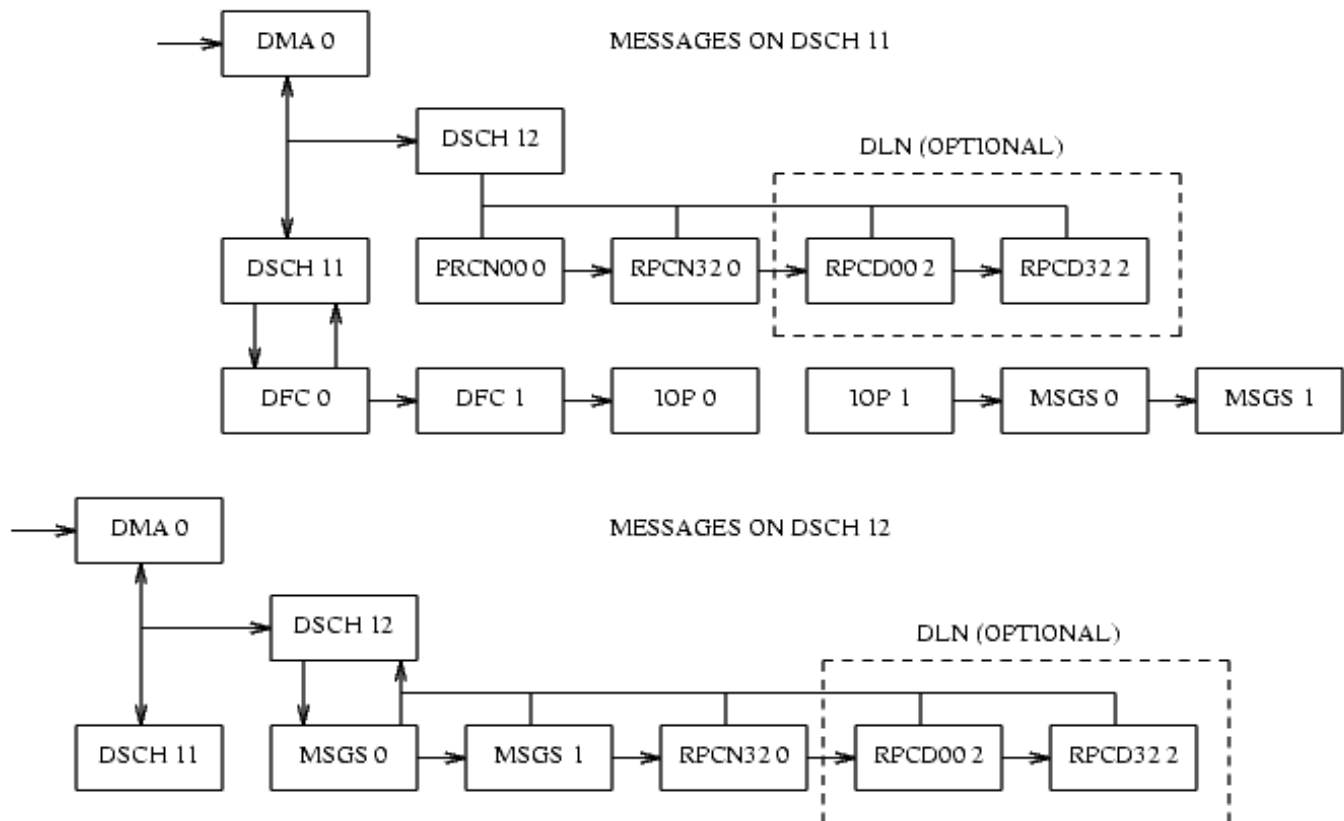


Figure 3.3-1 UCB Linkage (3B20D)

Refer to Figure 3.3-2 and check forms LN00 1, LN00 2, LN32 1, and LN32 2.

(1) To set the pointers for LN00 1:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **LN00**.
- At Field 4, (k_unit_number), enter **1**.
- The rest of the form is filled in.
- Go to Page 3 of the form
- There must be a side pointer to the DLN.
 - Field 44 must be **LN00**.
 - Field 45 must be **2**.
 - Field 49 must be **UNQD**.
 - Field 50 must be **0**.
- If these fields are not correct, make necessary changes and exit form.

(2) To verify the pointers for LN00 2:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **LN00**.
- At Field 4, (k_unit_number), enter **2**.
- Response: the rest of the form is filled in.
- Go to Page 3 of the form.
- There must be a side pointer to another LN:
 - Field 44 must be **LN00**.
 - Field 45 must be **3**.
 - Field 49 must be **UNQD**.
 - Field 50 must be **0**.
- If these fields are not correct, make necessary changes and exit form.

(3) To verify the pointers for LN32 1:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **LN32**.

- At Field 4, (k_unit_number), enter **1**.
- Response: The rest of the form is filled in.
- Go to Page 3 of the form.
- There must be a side pointer to the DLN:
 - Field 44 must be **LN32**.
 - Field 45 must be **2**.
 - Field 49 must be **UNQD**.
 - Field 50 must be **2**.
- If these fields are not correct, make necessary changes and exit form.

(4) To verify the pointers for LN32 2:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **LN32**.
- At Field 4, (k_unit_number), enter **2**.
- Response: The rest of the form is filled in.
- Go to Page 3 of the form
- There must be a side pointer:
 - Field 44 must be **LN32**.
 - Field 45 must be **3**.
 - Field 49 must be **UNQD**.
 - Field 50 must be **2**.
- If these fields are not correct, make necessary corrections and exit form.

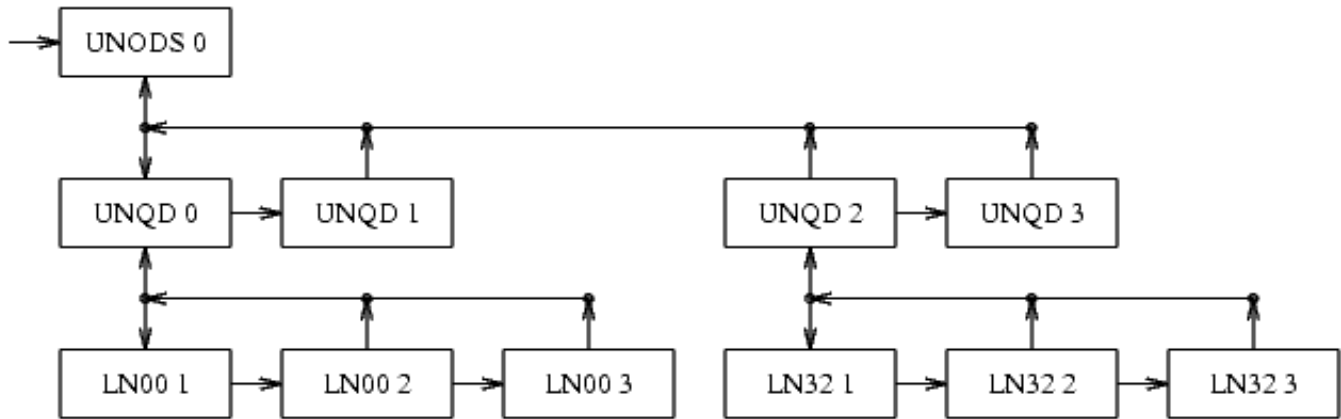


Figure 3.3-2 IUN Complex (3B20D)

3.3.4.3 Verifying Pointers in Required Unit Control Block (UCB) Forms (3B21D)

The pointers in each of the UCB forms should be checked. If the CNI is equipped with a DLN, it is important to verify that the pointers on all related UCB forms include the DLN.

Referring to Figure 3.3-3, check forms RPCN32 0, RPCD00 2, and RPCD32 2 to verify that the proper pointers exists.

(1) To verify the pointers for RPCN32:

- At Fields 1 and 2, hit the carriage return.
- At Field 3, (k_unit_name), enter **RPCN32**.
- At Field 4, (K_unit_number), enter **0**.
- The rest of the form is filled in.
- Go to Page 3 of the form.
- There must be a side pointer to the DLN:
 - Field 44 must be **RPCD00**
 - Field 45 must be **2**.
- If these fields are not correct, make these changes and exit the form.

(2) To verify the pointers for RPCD00:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **RPCD00**.
- At Field 4, (k_unit_number), enter **2**.
- The rest of the form is filled in.
- Go to Page 3 of the form

- There are no pointers, fields 44 and 45 are blank.
- The control pointers must exist as follows:

FIELD	ENTRY	FIELD	ENTRY
46	cntrl_0	47	CU
48	0	49	CH
50	14	51	cntrl_1
52	CU	53	1
54	CH	55	14

- If these fields are not correct, make the changes and exit the form.

(3) To verify the pointers for RPCD32:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **RPCD32**.
- At Field 4, (k_unit_number), enter **2**.
- Response: The rest of the form is filled in.
- Go to Page 3 of the form.
- There are no pointers, Fields 44 and 45 are blank.
- The control pointers must exist as follows:

FIELD	ENTRY	FIELD	ENTRY
46	cntrl_0	47	CU
48	0	49	CH
50	12	51	cntrl_1
52	CU	53	1
54	CH	55	12

- If these fields are not correct, make these changes, then exit the form.

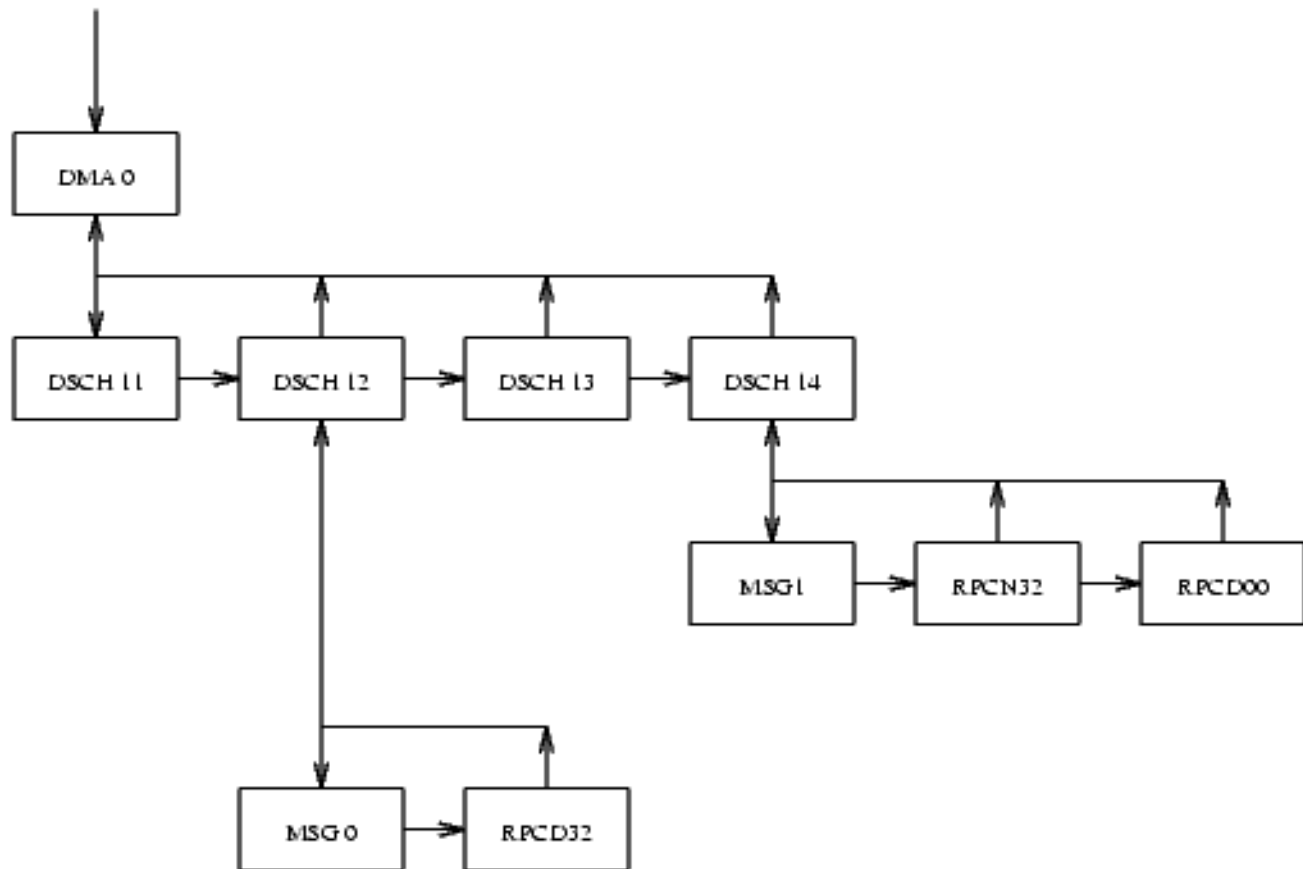


Figure 3.3-3 UCB Linkage (3B21D)

Refer to Figure 3.3-4 and check forms LN00 1, LN00 2, LN32 1, and LN32 2.

(1) To set the pointers for LN00 1:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **LN00**.
- At Field 4, (k_unit_number), enter **1**.
- The rest of the form is filled in.
- Go to Page 3 of the form
- There must be a side pointer to the DLN.
 - Field 44 must be **LN00**.
 - Field 45 must be **2**.
 - Field 49 must be **UNQD**.
 - Field 50 must be **0**.

- If these fields are not correct, make necessary changes and exit form.

(2) To verify the pointers for LN00 2:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **LN00**.
- At Field 4, (k_unit_number), enter **2**.
- Response: the rest of the form is filled in.
- Go to Page 3 of the form.
- There must be a side pointer to another LN:
 - Field 44 must be **LN00**.
 - Field 45 must be **3**.
 - Field 49 must be **UNQD**.
 - Field 50 must be **0**.
- If these fields are not correct, make necessary changes and exit form.

(3) To verify the pointers for LN32 1:

- At Fields 1 and 2, hit carriage return.
- At Field 3, (k_unit_name), enter **LN32**.
- At Field 4, (k_unit_number), enter **1**.
- Response: The rest of the form is filled in.
- Go to Page 3 of the form.
- There must be a side pointer to the DLN:
 - Field 44 must be **LN32**.
 - Field 45 must be **2**.
 - Field 49 must be **UNQD**.
 - Field 50 must be **2**.
- If these fields are not correct, make necessary changes and exit form.

(4) To verify the pointers for LN32 2:

- At Fields 1 and 2, hit carriage return.

- At Field 3, (k_unit_name), enter **LN32**.
- At Field 4, (k_unit_number), enter **2**.
- Response: The rest of the form is filled in.
- Go to Page 3 of the form
- There must be a side pointer:
 - Field 44 must be **LN32**.
 - Field 45 must be **3**.
 - Field 49 must be **UNQD**.
 - Field 50 must be **2**.
- If these fields are not correct, make necessary corrections and exit form.

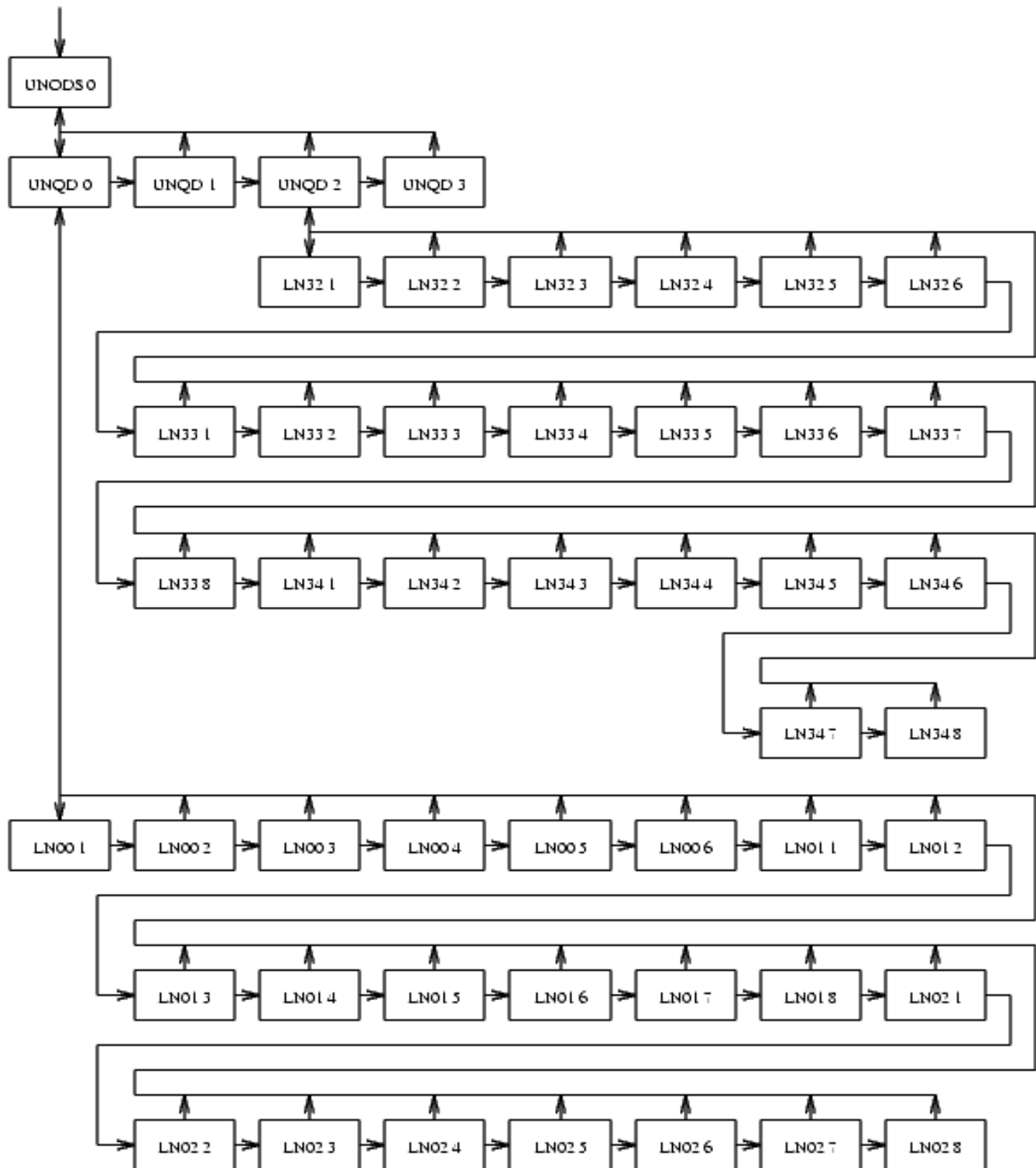


Figure 3.3-4 IUN Complex (3B21D)

3.3.5 Control Center Display Pages

Figures 3.3-5, 3.3-6, 3.3-7, 3.3-8, and 3.3-9 are examples of CNI MCC pages. For more details about these

pages please refer to 235-105-110, *System Maintenance Requirements and Tools*. (View the MCC Page Location Guide to find the exact section of the CNI page in the 235-105-110 document.)

SYS EMER
OVERLOAD

CRITICAL
SYS INH

MAJOR
AM

MINOR
AM PERPH

BLDG/PWR
OS LINKS

BLDG INH
SM

CKT LIM
CM

SYS NORM
MISC

118 - CHI RING STATUS

RING STAT: ACTIVE

STATUS

DSIG UNEQ

TSIG ACT

TCAP ACT

ALARMS

FAN ALM

FUSE ALM

PWR ALM

DISPLAY

1520 NODE STATUS

1521,GRP LINK STAT

1523 SUBSYSTEM STAT

GRP / MEM

0

1

2

3

4

5

6

7

8

34 NODE
LINK

33 NODE
LINK

32 NODE
LINK

02 NODE
LINK

01 NODE
LINK

00 NODE
LINK

+ACT

AVAL
IS

STBY

AVAL
IS

UNEQ

UNEQ

AVAL
IS

+ACT

AVAL
IS

ACT

AVAL
IS

UNEQ

UNEQ

AVAL
IS

+ RCPN

* DLN

INACCESSIBLE
POINT CODES

Figure 3.3-5 Example Page 118 Display - CNI Ring Status

SYS EMER OVERLOAD	CRITICAL SYS INH	MAJOR AM	MINOR AM PERPH	BLDG/PWR OS LINKS	BLDG INH SM	CKT LIM CM	SYS NORM MISC		
1520 - RING NODE STATUS									
RING STAT: ACTIVE				NODE<	RING	MAJOR	RI	NP	MAINT
				NODE NAME	POS	STATE	STATE	STATE	MODE
				01	RPC100 0	NORM	ACT	USBL	AUTO
				02	LN00 1	NORM	ACT	USBL	AUTO
				03	LN00 2	NORM	ACT	USBL	AUTO
				04	LN00 3	NORM	ACT	USBL	AUTO
				05	LN00 6	NORM	ACT	USBL	AUTO
				06					
				07					
				08					
				09					
				10					
				11					
				12					
				13					
				14					
				15					
				16					
CMD	FUNCTION								
2XX	RMV LN XX								
3XX	RST LN XX UCL								
400	BIS-EISO								
401/402	ALL NON-ACT (NEXT/PREV)								
403/404	ALL EQUIPPED (NEXT/PREV)								
500	DGN ISOLATED SEGMENT								
5XX	DGN LN XX								
6NN	DISPLAY GROUP NN								
7XX	RST LN XX COND								
(XX=LINE, NN=GROUP)									

Figure 3.3-6 Example Page 1520 Display - Ring Node Status

SYS EMER OVERLOAD	CRITICAL SYS INH	MAJOR AM	MINOR AM PERPH	BLDG/PWR OS LINKS	BLDG INH SM	CKT LIM CM	SYS NORM MISC

1521 - SIGNALING LINK SUMMARY GROUP 00

CMD	FUNCTION	OUTPUTS
200Y	RMV LN 00-Y	900 RING
300Y	RST LN 00-Y	901 LINKS
500Y	DGN LN 00-Y	

(Y=MEM)

	NODE NAME (GRP MEM)	FAR END CLLI	PROT TYPE	LINK TYPE	MATE NODE	MAJOR STATE	MINOR STATE	PRO RCVD
1	LN00 1	WASHDCSW77W	7	A	N/A	AVAL	IS	NO
2								
3	LN00 3	WASHDCSW77W	7	A	N/A	AVAL	IS	NO
4								
5								
6	LN00 6	WASHDCSW77W	7	A	N/A	AVAL	IS	NO
7								
8								

Figure 3.3-7 Example Page 1521 Display - Signaling Link Summary Group

SYS EMER OVERLOAD	CRITICAL SYS INH	MAJOR AM	MINOR AM PERPH	BLDG/PWR OS LINKS	BLDG INH SM	CKT LIM CM	SYS NORM MISC

1522 - SIGNALING LINK GROUP 00-1

CMD	FUNCTION	LOCAL STATES
2001	RMV LN 00-1	MAJOR : AVAL
3001	RST LN 00-1	MINOR : IS
5001	DGN LN 00-1	HDWR : IS
41001	MONITOR ON	
42001	MONITOR OFF	

NODE NAME: LN00-1
LINK PROTOCOL: 7

RECENT CHANGEABLE INFORMATION

ENCRYPTED : NOTENC	MATE : N/A	FAR END CLLI CODE : WASHDCSW77W
LINK TYPE : A	DIRECT LS : 001	FAR END FUNCTION NO : 0
]SPEED : 560	COMBINE LS : 002	FAR END POINT CODE : 123456789
FACILITY : MODEM	EC_MODE : BASIC	FAR END REGION NO : N/A
	TRANS MEDIUM : TERRESTRIAL	

Figure 3.3-8 Example Page 1522 Display - Signaling Link Group

SYS EMER OVERLOAD	CRITICAL SYS INH	MAJOR AM	MINOR AM PERPH	BLDG/PWR OS LINKS	BLDG INH SM	CKT LIM CM	SYS NORM MISC	
1523 - LOCAL SUBSYSTEM STATUS								
POINT CODE: 123456789				SUBSYSTEM NUMBER AND STATUS				
STATUS: AVAILABLE				0	1	2	3	4
				5	6	7	232	233
				234	235	236	237	238
				239	240	241	242	243
				244	245	246	247	248
				249	250	251	252	253
				254	255			

Figure 3.3-9 Example Page 1523 Display - Local Subsystem Status

3.4 CNI SYSTEM DIAGNOSTICS

3.4.1 Diagnostics Purpose

The CNI system diagnostics are performed both automatically and manually. Automatic diagnostics are performed by the automatic ring recovery. Diagnostic procedures for the CNI in the switch environment are covered in 235-105-220, *Corrective Maintenance Manual*.

The IMS and CNI diagnostics serve the following purposes:

- Fault detection and resolution:
 - May be invoked by manual request.
 - Invoked by error analysis program part of automatic ring recovery.
- Repair verification after maintenance tasks.

3.4.2 System Maintenance Interface

Local maintenance access and status information for the IMS and AM is obtained through video terminals and receive-only printers (ROPs). The MCC provides the primary interface and communications for system control and display, input and output messages, and the AM emergency action interface control display.

The ROP provides hard copies of the MCC input and output messages, report status information, fault conditions, audits, and diagnostic results.

3.4.3 Performing Diagnostics

Manual RN diagnostics input and output messages are entered and interpreted from the maintenance terminal. The *UNIX*® RTR operating system provides assistance to users in entering input messages by identifying invalid data in the user's message. Invalid values are rejected accompanied by an appropriate error acknowledgement. The user can obtain further help by entering a question mark (?). For further information on the diagnostic performance and message structure, see 235-105-220, *Corrective Maintenance Procedures*.

3.5 AUDITS

3.5.1 Description

Audits are a collection of programs to monitor the occurrence of errors and inconsistencies encountered in the application software. Some of the error types that audits look for are:

- Errors in the unit status (for example, a unit is reported to be out of service when it actually is in service).
- Errors that would cause messages to be lost when they are passed from one function to another.
- Application integrity errors (where jobs run too long or are prevented from being run).
- Errors in the consistency between tables.

Most audits detect and identify errors, and in some cases, correct the errors found. The most common error correction strategy to correct inconsistencies is to overwrite the conflicting version with the most reliable version. Other audits simply initialize the erroneous data. For more detailed information concerning audits, see 235-600-400, *Audits Manual*.

When the audit relates to the data base, it determines whether the related tables contain valid data, have been updated properly, and are consistent. If the error cannot be corrected by recent change, the audit corrects the problem at the time it is encountered, if possible. If it is not possible for the audit to correct the problem, the audit report contains detailed data on the error to enable the user to manually locate and correct the errors. For more information on specific messages and error codes, see 235-600-700, *Input Message Manual* and 235-600-750, *Output Message Manual*.

3.5.2 CNI Audits

3.5.2.1 Central Node Control Audit (AUD:CNC)

This routine audit is run automatically a number of times every hour. The purpose of the audit is to detect any inconsistencies or errors in the AM relating to the LNs. Internal ring node maintenance records are checked for inconsistencies which could prevent jobs from progressing, or to be unnecessarily shortened.

This audit normally takes less than 10 seconds to run, depending on the number of equipped nodes in the office.

3.5.2.2 Node State Audit (AUD:NODEST)

This routine audit is run automatically several times every hour. The purpose of the audit is to detect any inconsistencies in the data maintained in the IMS relative to the node state. The audit compares the node availability map with the IMS driver node state data. The node availability map indicates whether the node is available or not. The audit corrects any consistencies by copying the IMS driver data to the node availability map.

This audit usually takes about 2.5 minutes to run, depending on how busy the IMS is at the time.

3.5.2.3 Internal Data Audits (AUD:NIDATA)

The internal data audits compare the tables contained in the main memory with tables maintained on disk and report any mismatches. The tables are also checked for invalid data within a table and consistencies across the tables. The audit reports all errors that are found by using the appropriate AUD:NIDATA output message. The error code contained in the output message can be used to find the action to be taken to correct the problem.

The audits can run "on demand" by using the maintenance terminal, or as routinely scheduled audits by using the

equipment configuration data base, depending on how the equipment configuration data base has been set. This audit family includes member audits:

- NIDATA 1 — Office identification data
- NIDATA 2 — Link configuration data
- NIDATA 3 — Logical-physical translation data
- NIDATA 4 — SS7 routing data
- NIDATA 5 — Subsystem information data
- NIDATA 8 — Global title translator data
- NIDATA 10 — Protocol Timer/Parameter data.

Any audit member may be set up for routine or manual operation. It is recommended that these audits be run after the completion of recent change activity.

3.5.2.3.1 Routine Operation

To schedule the audits to run in the routine mode, enter the following command at the maintenance terminal:

```
EXC:ENVIR:UPROC,fn="/no5text/cni/proc/niauds.on"
```

This command schedules the audits to execute at the recommended interval of once a day at 7:00 a.m.

To unschedule the audits, enter the following command at the maintenance terminal:

```
EXC:ENVIR:UPROC,fn="/no5text/cni/proc/niauds.off"
```

NOTE: The audit activating process requires 3 to 5 minutes to run. The actual run times of the audits may vary, depending on the system load.

3.5.2.3.2 Manual Operation

To schedule the audits to run the manual mode, enter the following command on the maintenance terminal:

```
AUD:NIDATA=x
```

Where x represents the specific audit member to be run, 1 through 5, 8, or 10 (see "Internal Data Audits," Section 3.5.2.3).

3.5.3 Remote Access Subsystem (REMACS) Audit (EXC:REMACS)

This routine audit is run automatically. However, it can be run on demand through the maintenance terminal.

The purpose of this audit is to assure consistency between the data in the remote nodes and the data in the AM. The data is divided into "windows." A window is a consecutive area of memory consisting of one or more bytes. Remote Access Subsystem provides an audit of each window. The two sets of data are audited on a byte-to-byte comparison. If the data does not match, the data in the node is audited a second time, and if the second audit fails, the data is updated. The erroneous data in the nodes and the current data in the AM are printed on the receive-only printer. The data comparison is made on all auditable windows each time the audit is invoked. An auditing cycle is completed when all windows for all nodes are audited.

NOTE: Unlike the other audits mentioned, this is an internal running audit that is not controlled by the system integrity monitor (SIM) and has no Equipment Configuration Data (ECD) forms associated with it. However, the `exc:remacs` command does allow audit control much like the ECD forms.

3.5.4 Network Management Audit (AUD:NMDATA)

This is a System Integrity Monitor controlled segmented audit that is part of the Signaling Link Monitor Kernel (SLMK) process, and is the name of the group of audits concerned with the integrity of the network management dynamic data. The equipment configuration data base (the audit execution interface) is used to define the different characteristics of the audit. The audit can run "on demand" by using the maintenance terminal, or as a routinely scheduled audit by using the equipment configuration data base, depending on how the equipment configuration data base has been set. This audit family presently has two member audits as follows:

- The routing data linked list and consistency check audit
- The loadshare tables audit.

The Audit Members may be run in either the "error detection" mode, or "error correction" mode. The mode is specified by the equipment configuration data base. During the normal CNI operation, the point code state changes (for example, from accessible to inaccessible). These changes are reported to the applications by using SS7 reports transaction. During the Audit Member 1 execution, no SS7 reports transactions are generated. So, it is recommended that the equipment configuration data base be programmed to specify that Audit Member 1 always run in the "error detection" mode.

The applications that have CNI routing data maintained in processors other than the AM, perform remote copy of the data and are updated by the remote access subsystem when Audit Member 1 or 2 changes the data while executing the "error correction" mode.

When the detailed report (DETL) function is set in the equipment configuration data base, a report is issued for each error found followed by an audit completion message. The detailed report identifies the following:

- (1) Where the error occurred
- (2) The erroneous data value
- (3) Application table index
- (4) The correct data value.

When the summary (SUM) report function is set in the equipment configuration data base, only the audit completion message is displayed. The default value is DETL which displays the entire report.

Audit Member 1 (NMDATA 1):

This audit member is designed for checking six tables for error conditions in the dynamic routing information. These six tables are used for managing the dynamic routing data as network events occur; such as, remote link failure or congestions. Discrepancies between fields in the routing table entries are also audited.

Audit Member 2 (NMDATA 2):

This audit member is used for auditing loadshare table data. The data is used for message routing link selection in the direct link node (DLN) and the AM. The update to the master version of the DLN copies is similar to the Audit Member 1. However, in Audit Member 2, if a change is made in the master copy of the table, an SS7 loadshare table update report is sent to the application. Audit Member 2 can be run in the "error correction" mode with no side effects.

Any audit member may be set up for routine or manual operation.

Routine: To schedule the audit to run in the routine mode, the equipment configuration data base must specify either:

- Timed audit
- Frequency group audit.

Once the equipment configuration data base is set up, the Switch Integrity Monitor automatically schedules the audit. In this mode, the audit does not produce an output, if no errors are found.

Manual: To schedule this audit in the manual mode, enter the following MML command on the maintenance terminal:

```
AUD:NMDATA=x
```

Where x represents the specific Audit Member to be run, 1 or 2.

The audit adheres to the guidelines for segment length or the kernel process audits. It takes approximately 30 minutes to complete the **NMDATA 1** in the routine mode in frequency group C, and approximately 3 minutes to complete in the manual mode under lab conditions. Actual run times may vary, depending on the size of the tables and current network status.

NOTE: Customer Technical Support (CTS) should be on line when executing the audit in error correction mode.

3.5.5 Link And Band Status Audit (AUD:LKBDST)

The Link and Band Status Audit is a routine audit that is used to detect and correct any inconsistencies or errors in the basic link and band status information maintained by both the central processor and the nodes. This data consists of a link state, a node state, an internal link and mate link status (indicates if the link or its mate is carrying traffic or not), route switch status (reflects band status), and various other node parameters and indicators. If the link is SS7 type and has virtual links assigned, this data consists only of ECIS routing data (for example, the point code routing data, SS7 node parameters, and SS7 link status data are not checked).

The Link and Band Status Audit can be run in either automatic or manual mode. In the automatic mode, the audit is run automatically several times a day (depending on the number of equipped nodes). Each equipped node (except RPC nodes) are audited in sequence until all nodes in the office have been checked. Each time LKBDST executes, one node is audited. On the next invocation, the audit continues with the next node. If a node is out of service, it is skipped. In the manual mode, either a specified node or all nodes can be audited. In the manual mode, this audit can be run by an input message.

The central processor sends a query to the node being audited. The node responds by sending the data described in the two previous paragraphs to the central processor (from one to three messages are required) to be compared with basic link and band status information in the central processor. This data consists of correctable and noncorrectable data.

Link states and route switch status are correctable. If a correctable error is found, the central processor sends another message to the node with the proper data. Any one error causes all correctable data to be updated.

The link status, mate link status, and node states are noncorrectable. If a noncorrectable error is found, the node is restarted (for example, it is diagnosed and downloaded).

NOTE: If the audit is executing manually on all nodes, to avoid removing a large number of nodes from service

simultaneously, the audit aborts if more than two nodes must be restarted.

Input and output messages are described in the 235-600-700, *Input Message Manual* and the 235-600-750, *Output Message Manual*. If the audit is running automatically or the detailed option (DETL) was input, up to 16 detailed reports are provided. If more than 16 errors are found, a modified form of the raw data report is used to indicate the number of errors found and the number of errors corrected.

This audit completes within 15 minutes to 2 hours of elapsed time, depending on how busy the office is at the time and the number of equipped nodes in the office. This audit corrects all errors found by one of the methods described earlier.

3.5.6 AUDIT CONTROL SYSTEM

3.5.6.1 Makeup Of Audit Control System

The audit control system consists of the following:

- **System Integrity Monitor (SIM)** - Software integrity and audit control process. The SIM is responsible for scheduling and dispatching all audits.
- **Equipment Configuration Data Base (ECD)** - The software integrity records in the ECD contain information about the execution of audits and audit error recovery.
- **Output Formatter** - This provides a consistent output message format when reporting audit results to the user.
- **Audit Commands** - *UNIX*® RTR operating system input commands (`STOP:AUD`, `OP:AUD`, `OP:AUDERR`, `INH:AUD`, and `ALW:AUD`) are provided to query and request software integrity services. Both CNI and *UNIX*® RTR operating system input commands are provided to run specific audits.
- **Audit Requests** - These are requests from other processes to run audits. These are automatically generated audits invoked by other trouble-clearing software.
- **Plant Measuring Interface** - Counts of audit attempts and failures are stored in the plant measurements data base and appear on the Plant Measurement Count Report (PMCR) generated hourly.

Audit execution information is reported to the user by using the `AUD` output messages. There are, however, other messages that give important audit information to the user as discussed in the following paragraphs.

3.5.6.2 Plant Measurement Count Report

The plant measurement count report is generated by the *UNIX*® RTR operating system, both hourly and daily. The section of the report, under system performance, details the audit activity for the preceding hour. Two items are listed for each audit as follows:

- The number of times the SIM attempted to run the audit
- Number of errors detected.

The actual number of successful completions of the audit and the number of errors corrected must be obtained from the `AUD` output message, or from the `OP:AUD` command message. If an audit is included on the PMCR report, it is in the equipment configuration data base and has attempted to run. Each scheduled audit should appear on the PMCR at least once each day. For further information about the PMCR, refer to the 235-600-750, *Output Message Manual*.

3.5.6.3 OP-AUD

This output message is generated in response to a manual request `OP:AUD`. This output contains the status of specified audits controlled by the SIM. There are three possible actions that can be taken on the basis of the `OP-AUD` report as follows:

- Stop audits that must be stopped.
- Inhibit audits from running routinely.
- Allow audits to run routinely.

3.5.6.4 OP-AUDERR

This report is generated in response to the manual request `OP:AUDERR` requesting error counts that were executed from the ECD for audits controlled by the SIM. This report simply furnishes statistical information, and no action is required.

3.5.6.5 REPT AUDSTAT

This output message is generated automatically by the system approximately every 30 minutes, when one or more audits are inhibited or blocked. The report identifies inhibited or blocked audits controlled by the SIM. The user can take the following actions:

- Obtain additional status on inhibited audits.
- Allow audits that were previously inhibited to run routinely.

3.5.6.6 REPT SIMCHK

The `REPT SIMCHK` output message is generated to report failures in the SIM. Some of the conditions that cause this report to be generated are as follows:

- If the audit manager fails to initialize after a system boot, the SIM temporarily inhibits all audits and outputs this message.
- If the SIM has difficulty accessing the ECD when routinely running audits, this message is generated.
- If the SIM cannot allow audits to run within 5 minutes, it generates another output message.

Manual action is required by the user to determine the cause of the problem that caused the `REPT SIMCHK` message to be generated.

3.6 PROCESSOR RECOVERY MESSAGES

Two processor recovery messages (PRMs) contain some audit related information to the user during the AM recovery. Both of these PRMs output information that describes a function or possible error and corrective action that should be taken.

Inconsistencies or errors in the status of various scheduled jobs related to IUNs in the AM are detected by the Central Node Control Audit (AUD:CNC). This is an automatic routine audit that is run several times every hour.

3.6.1 Failure PRM

During recovery, the CNI initialization process produces a failure PRM. The PRM is displayed on the master control center (MCC) and the ROP. The first failure PRM is selected by the emergency action interface PRM-TRAP option and displayed in reverse video (dark characters on light background) on the MCC. See 235-600-601, *Processor Recovery Messages Manual* for more details on the processor recovery messages.

The failure PRM identifies the process encountering the failure, the reason for the failure, and sometimes other failure data. The basic format of a PRM is shown in Figure 3.6-1.

3.6.2 Definition of PRM Digits

The following (See Figure 3.6-1) are definitions of the information represented by the digits in the PRM messages:

Z	=	Zero (0) for control unit 0 (CU0).
		One (1) for CU1.
Digit 0	=	Message type: F = Failure E = Success A PRM message is designated with a failure (F) when an error is considered fatal. A success PRM (E) message gives information describing a function or a possible error and any corrective action required.
Digit 1	=	Major step or process that output the PRM. Normally, the entry for this digit is an E for application process. If the digit is not an E, refer to the <i>UNIX</i> ® RTR operating system.
Digit 2	=	<i>UNIX</i> ® RTR operating system level of initialization.
Digit 3	=	Application level of initialization.
Digits 4 & 5	=	Two-digit code for process identifier. The CNI PRM digits are as follows: 7F = CNI Initialization (CNINIT) process. 8F = CNINIT process.
Digits 6 & 7	=	Two-digit hexadecimal code for the function number. Each function of each process is numbered.
Digits 8 & 9	=	Two-digit code that identifies the error within the function where the error occurred. Each error of each function is numbered.
Digits 10 & 11	=	Two-digit code identifying the internal state of the originating process at the time of the error.
Digits 12 & 13	=	Two-digit code identifying the state of the process just before the time the error occurred.
Digits 14 & 15	=	Two-digit code used to represent data about the error. These digits are not always used. Table 3.6-1 contains the CNIINIT child process and PRDEX identifiers that may appear in this field. Table 3.6-2 provides the CNIINIT default audit values.
Digits 16 - 21	=	The hardware status of the AM when the PRM was generated.

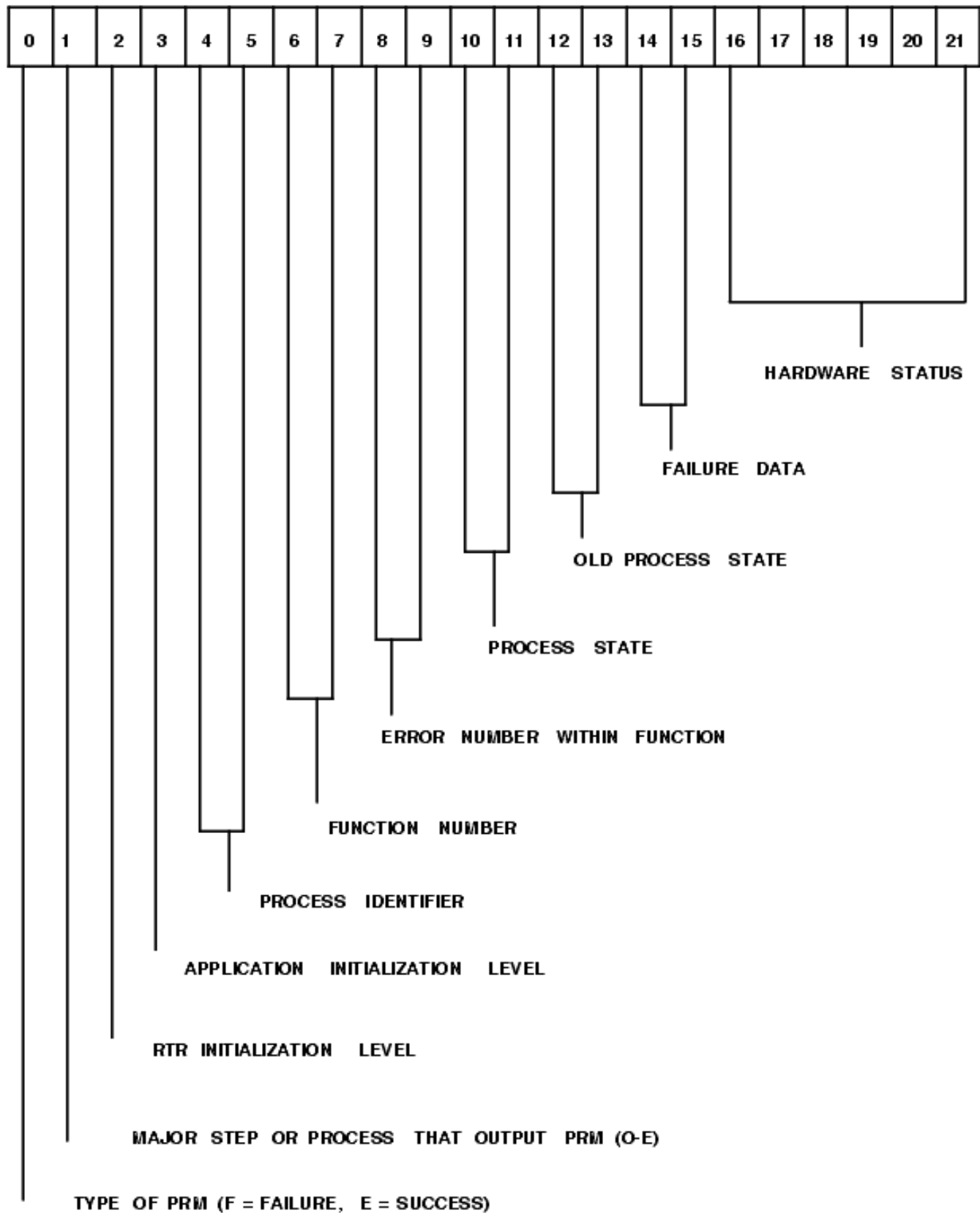


Figure 3.6-1 Processor Recovery Message Format

Table 3.6-1 PRM Digits 14 and 15 CNIINIT's Child Process Creation

VALUE OF CHILD_NUM, INDEX, OR PRDEX	PROCESS NAME
0	N/A
1	CMMSADM
2	N/A
3	imsdrv.p
4	SLMK
5	CNIER
6	CNISNM
7	CMMSDP
8	MON TRAP
9	OMAP
10	cdp
11	RGP_PRT

Table 3.6-2 PRM Digits 14 and 15 CNIINIT's Default Audit

VALUE OF AUDEX	FAMILY NAME	MEMBER NUMBER	INSTANCE NAME
0	N/A	N/A	N/A
1	NIDATA	NIDATA	NIDATA

3.6.3 Sample Processor Recovery Message

Following is an example PRM and field explanations.

- **PRM:** FE_{xy} 7F1E eess oddd hh hh hh
- **RECOVERY STEP:** CNI initialization process
- **FUNCTION:** CNI boot initialization
- **DESCRIPTION OF FIELDS**

FE F = Failure, E = Successful.

x This entry is the RTR initialization level.

y This entry is the application initialization level.

7F This indicates that the PRM originated from the CNIINIT process.

ee The indication here is the error number within the function. These may be as follows:

- 01 - An unknown process terminated, `ms_ident (i)` is invalid.
- 02 - This process died before reaching the RUNNING state.
- 03 - A critical process termination occurred during initialization.
- 04 - Bad data in the process table `rc_type` is invalid.

ss The entry here indicates the state of the CNIINIT when the error was detected.

oo The previous state of the CNIINIT subsequent to the state in which the error was detected.

dd This field contains the value of `i`. The variable `i` is an index into CNIINIT's child process creation table.

hh

These are hardware status digits.

- **EXPLANATION:** This type of PRM indicates that the CNI child process terminated during a boot initialization. Field dd can be used to determine the terminated process.

The 235-600-601, *Processor Recovery Messages User's Guide* provides more complete explanation of the PRMs and their meanings.

3.7 CNI SYSTEM RECOVERY

3.7.1 CCS Transport Initialization And Recovery

Both CNI and IMS support several levels of initialization, with each level offering a different tradeoff between thoroughness and the amount of impact on the application. The actions that take place during each level is described here, with attention to those which directly affect communication between the AM and the CNI ring and, therefore, affect the ability to make CCS calls.

The escalation of one initialization level to a more severe level as a result of errors is a part of the recovery strategy of both of these subsystems. These events are also briefly documented here.

The CNI system recovery can be initiated either from within CNI/IMS on the detection of errors, or from the application integrity monitor (AIM) process. Responsibility for the overall CCS initialization can be said to reside within the AIM, RINGMON, and CNIINIT processes.

The purpose of RINGMON is to monitor maintenance events from the CNI ring. The purpose of CNIINIT is to create and initialize all CNI processes and the IMS driver (IMSDRV) process. RINGMON and CNIINIT communicate directly with AIM during any CNI initialization.

Manual initialization of the CCS transport can be achieved with either an AM boot, or by using the `INIT:CNI` input command. Not all levels of initialization cause CNIINIT to "abort and boot," as is explained in the following sections.

3.7.2 CNI/IMS Initialization Strategy

The CNI/IMS initialization is controlled by the CNIINIT process which is created, monitored, and sequenced by AIM. The AIM process does not interface directly with IMS. The CNIINIT is responsible for software recovery actions involving CNI processes and the IMS system as a whole.

The CNIINIT creates the CNI processes and IMSDRV during a CNI boot level initialization. The IMSDRV, in turn, creates all other IMS processes. During non-boot levels of CNI initialization, CNIINIT controls the sequence of software resynchronization within CNI processes and IMSDRV.

3.7.3 CNI Levels Of Initialization

The following describes the different CNI levels and their impact.

CNI Level 0: The CNI level 0 is not an actual initialization. The CNI and IMS audits are invoked. The audits can be run automatically by CNI or IMS processes, or they can be requested by the input message, `INIT:CNI, LVL0;`. There is no CCS outage associated with a CNI level 0.

CNI Level 1: The CNI level 1 causes all CNI data tables to be rebuilt from information in the AM and the CNI ring, as required. The manual input command `INIT:CNI, LVL1;` causes a CNI level 1 to occur, and also invokes an IMS 1B initialization (see next section). This level of initialization causes a CCS transient call outage of about 10 seconds. The CNI level 1 can be automatically requested by the software, when errors are detected.

CNI Level 2 (FPI): During a CNI level 2 full process initialization (FPI), the critical CNI and IMS processes do not abort. They initialize their internal variables to a "safe" point, and close and reopen their IMS communication channels. The CNI ring resynchronization takes place. Noncritical CNI and IMS processes are killed and recreated. The manual input command `INIT:CNI, LVL2;` causes a CNI level 2 FPI to occur, and results in about 12 seconds of CCS outage. The same level may also occur as a result of automatic software recovery.

CNI Level 2 (Boot): The CNI level 2 boot initialization causes all CNI and IMS processes to abort and be recreated. The CNI ring is resynchronized. This level of initialization cannot be requested by an input command, but it is performed whenever an RTR level 2 (manual or automatic) is performed. It may also be requested from within the

CNI/IMS software, when a level 2 FPI is unsuccessful.

CNI Level 3: The CNI level 3 initialization, like the level 2, causes all CNI and IMS processes to abort and be recreated. In addition, CNI zeroes its PAS area and reads in the PAS data from disk. The CNI also downloads routing data from the AM to the nodes. The manual input command `INIT:CNI,LVL3;` requests a CNI level 3 initialization; the CCS outage duration is about 30 seconds. The CNI level 3 also takes place during manual or automatic RTR level 3 initializations.

CNI Level 4: The CNI level 4 initialization is a complete boot of the CNI/IMS system. It causes all CNI and IMS processes to abort and be recreated. It causes CNI's PAS area to be reinitialized. It also causes all text and data to be downloaded to the nodes. The manual input command `INIT:CNI,LVL4;` causes a CNI level 4 initialization to take place. The CCS outage is less than two minutes. A manual RTR level 4 with certain input parameters (42-p-54, 42-9-54, and retrofit parameters on the EAI page) causes a CNI level 4 to occur as part of the requested boot.

3.7.4 IMS Levels Of Initialization

The IMS subsystem supports six levels of initialization: levels 0, 1A, 1B, 3 (FPI), 3, and 4. The three lower levels (0, 1A, 1B) can be requested internally by IMS.

IMS Level 0: The IMS level 0 initialization is simply for running audits. Access to the message switch is maintained. The audits take corrective action if problems are found.

IMS Level 1A: An IMS level 1A causes initialization of communication between the AM and the RPCs. Audits are run, and communication among IUNs is maintained. The CCS calls complete because the IMS message switch in the AM is still available. The IMS 1A is typically requested whenever an RTR level 1 (51) is performed, in which case it is done without a CNI initialization. However, if the IMSDRV process detects that it was on the kernel stack when an RTR level 1 occurred, it causes an IMS level 1B and a CNI level 1 initialization.

IMS Level 1B: An IMS level 1B stops the message switch and reinitializes it, causing messages to be lost. Communication between the AM and the DLNs is initialized, as well as communication between the AM and the RPCs. The IMS user processes must close and reopen channels. The IUNs can still communicate with each other during a level 1B. The IMS level 1B is performed when a manual CNI level 1 is requested.

IMS Level 3 (FPI): The IMS level 3 full process initialization parallels the CNI level 2 FPI. The IMS critical processes reinitialize their global variables and communication channels, but they do not abort. The IMS level 3 FPI occurs during an automatic or manual CNI level 2 FPI.

IMS Level 3: The IMS level 3 involves aborting and recreating all IMS processes in the AM. The IMS determines the usable ring configuration. The CNI may call for IMS to download selected ring nodes. The IMS level 3 occurs during any CNI level 2 boot or CNI level 3 initialization.

IMS Level 4: The entire IMS subsystem is initialized during an IMS level 4. The IMS determines the ring configuration by performing functional tests. Program and data files are downloaded to all nodes. The IMS level 4 occurs during any manual or automatic CNI level 4 initialization.

3.7.5 Escalation Limits

The following rules govern the escalation within the CNI/IMS system:

- There is no escalation based solely on the number of manual initializations performed within a time interval.
- Failure of a critical audit during a CNI level 0 initialization escalates to a CNI level 1 initialization. Likewise, IMS level 0 initializations may escalate to IMS 1A.

- Failing initializations escalate to successively higher levels. For instance, a failing CNI level 2 FPI escalates to a CNI level 2 boot.
- Automatic CNI levels of initialization can be requested by RINGMON, as well as from within CNI.
- The AIM process controls escalation of automatic CNI recovery actions requested by RINGMON. For example, after the threshold of automatic CNI level 1 initialization is exceeded, AIM escalates the next request to a CNI level 2 FPI.
- The AIM controls the CNI level performed during an RTR initialization. The highest level of automatic escalation is a CNI level 4 initialization.
- The CNI can internally escalate a CNI level 2 FPI to a CNI level 3. This occurs when CNI detects corruption of the PAS data area, which can only be recovered during CNI levels 3 and 4.
- During any CNI initialization, if RINGMON detects that the DLNs have not been successfully initialized by CNI/IMS, RINGMON immediately requests escalation to a CNI level 4 initialization. This insures that all nodes, including the DLNs, are downloaded and restarted.
- The RTR software check inhibits, if turned on, prevents CNI initializations from escalating to AM initializations.

3.8 CNI/IMS INHIBITS AND CRITICAL NODE RESTORE

3.8.1 Hardware And Software Inhibit

The Hardware - Software Inhibit feature provides the capability of limiting IMS and CNI recovery actions when some hardware or software problems occur. The feature is useful in "quieting down" a machine that is rolling in recoveries of one form or another to allow switch personnel to take manual control.

The overriding purpose of system inhibits is to prevent thrashing in the face of certain kinds of error conditions which would otherwise adversely impact system operation. The automatic detection of system trouble is highly desirable to quickly and reliably restore system operations to normal. However, repeated non productive recovery attempts may interfere with optimum system operation in special circumstances.

Two forms of inhibits are possible:

- Software (SW) - to prevent escalation of software recovery actions where the higher action is taken arbitrarily (that is, based upon threshold counts). Low level actions may still be permitted.
- Hardware (HW) - to disable hardware check circuits to blind software to a recovery stimulus. This type of inhibit is especially effective for false error detectors (parity errors).

With inhibits enabled, the system has limited automatic recovery capabilities, and therefore **must** be attended by office personnel as a subsequent system error will likely require manual action. Inhibiting system checks in a healthy system should **not** affect system operation.

Even if recovery actions are blocked due to inhibits or unsuccessful retries, the system should eventually restore itself to normal after the original problem is cleared (unless cleared earlier by switch personnel).

When software inhibits are turned on for an office CNI initialization, levels 2 through 4 will not escalate unless manually requested. To prevent process thrashing, the retry of an initialization is delayed as follows:

- one minute delay after five CNIINIT failures within fifteen minutes,
- one minute delay after four RINGMON failures within fifteen minutes,
- five minutes delay after one more failure, and
- fifteen minutes delay after yet another failure,

Any subsequent failures within fifteen minutes causes another fifteen minutes delay.

This delay schedule is decremented once each fifteen minutes. In other words, if the delay were at fifteen minutes and there were no initializations for thirty minutes, the delay would be reset to one minute.

3.8.2 CNI Critical Node Recovery Monitor (CCM)

The CNI part of the Critical Node Restore feature is known as the CNI Critical Node Recovery (CNR) Monitor or CCM for short. The CCM feature monitors the states of SS7 or CCS6 link nodes and direct link nodes and looks for combinations of failures that severely impact the system. When severe and critical failures are found, it initiates emergency recovery actions aimed at restoring the basic signaling and processing capability as quickly as possible.

3.9 DATA ADMINISTRATION (RECENT CHANGE AND VERIFY)

3.9.1 Introduction

This section covers the procedures for populating the common network interface (CNI) data base with Common Channel Signaling (CCS) message routing capability for each of the CCS feature services. The routing and CNI data base setup information is described for the CCS features and for application in the Signaling System 7 (SS7) recent change implementation.

3.9.2 CCS Routing Capabilities For CCS Features

3.9.2.1 ISUP and Number Service CCS Routing

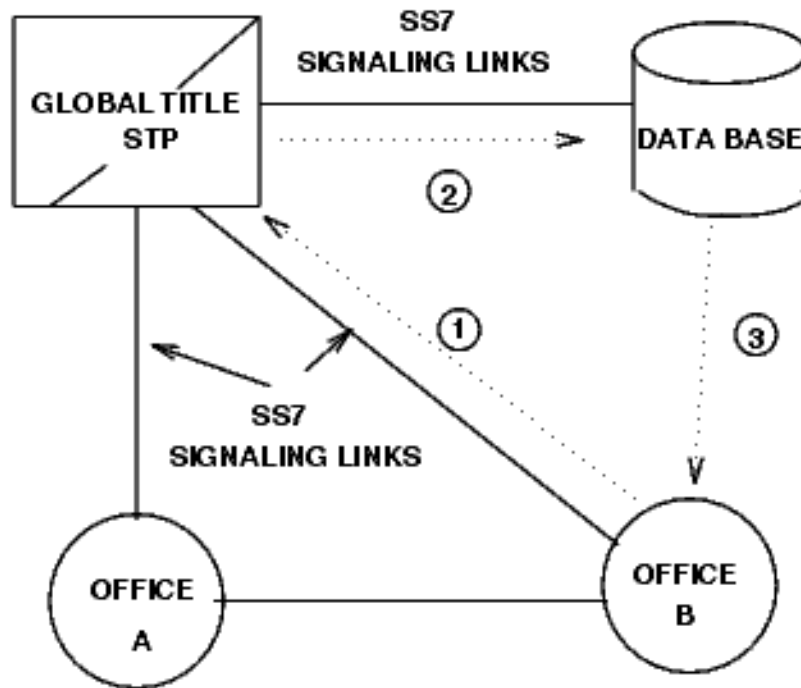
The SS7 signaling protocol routes messages through the CCS network for the ISDN User Part (ISUP) trunking feature and for the number service features [Service Switching Point 800 (SSP800) and Local Area Signaling Service (LASS)]. The SS7 messages for the ISUP trunking feature are routed through the network based on the destination point code (DPC) at the far-end of the trunk group. The SS7 messages for the transaction capability application part (TCAP) features, called signaling connection control part (SCCP) messages, are routed through the network based on the DPC and subsystem number (SSN) of the signaling service or by a "global title." The SSN identifies the specific feature within a switch or data base that should process the message.

Figure 3.9-1 is an example of the basic signaling network architecture showing the global title routing for SSP800, LASS, line interface data bus (LIDB), channel-associated signaling (CAS), and ISUP.

3.9.2.2 Global Title Routing

The address in the global title SS7 message does not contain sufficient information to route the message to its final destination. For SCCP (for example, SSP800 and LASS), a pair of signaling transfer points (STPs) are chosen to translate the global title address into a new DPC and SSN destined for the appropriate data base (SSP800) or office (LASS).

Global title messages originated from the switch contains only sufficient information to route the message to the STPs chosen to perform global title translations. These messages are marked for global title translation to be done upon arrival at the STPs.



1. END OFFICE B SENDS GLOBAL TITLE SSCP MESSAGE TO GLOBAL TITLE STP
2. AFTER GLOBAL TITLE TRANSLATION, THE STP SENDS SSCP MESSAGE TO THE DATA BASE USING DESTINATION POINT CODE AND SUBSYSTEM NUMBER OF DATA BASE.
3. THE DATA BASE REPLIES TO THE QUERY WITH SSCP MESSAGE ROUTED BACK TO THE END OFFICE USING DESTINATION POINT CODE AND SUBSYSTEM NUMBER OF END OFFICE B.

Figure 3.9-1 Global Title Routing for SSP800, LASS, Line Interface Data Bus (LIDB), and ISUP

Information is contained in the global title STPs data bases to determine where to route the message; to a data base for SSP800 or to an office for LASS. The global title message from the switch contains the global title translation type corresponding to the specific feature and six customer dialed digits (Figure 3.9-2). The global title STPs use this information to reformat the message with the DPC and SSN of the chosen (SSP800) data base or (LASS) office (Figure 3.9-3). When the information message is routed to the proper destination, the reply is generated back to the switch using the DPC and SSN of the switch in the calling party address of the original message (Figure 3.9-4).

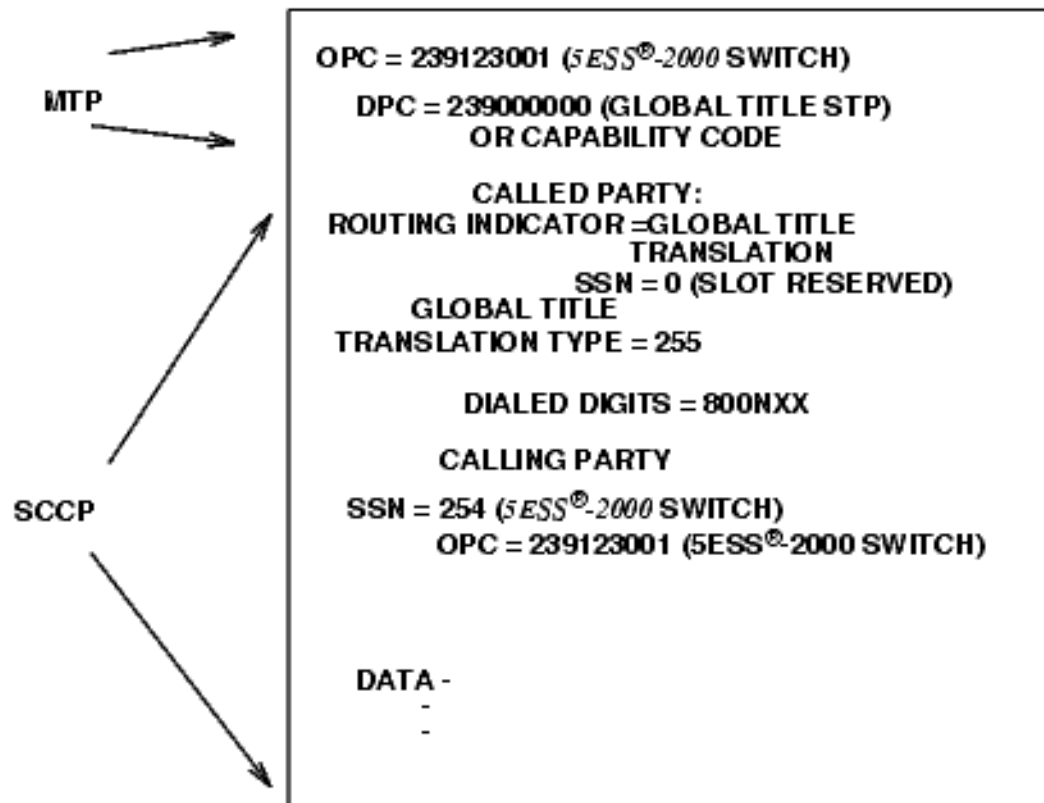


Figure 3.9-2 Query to CCS Network (Global Title STP)

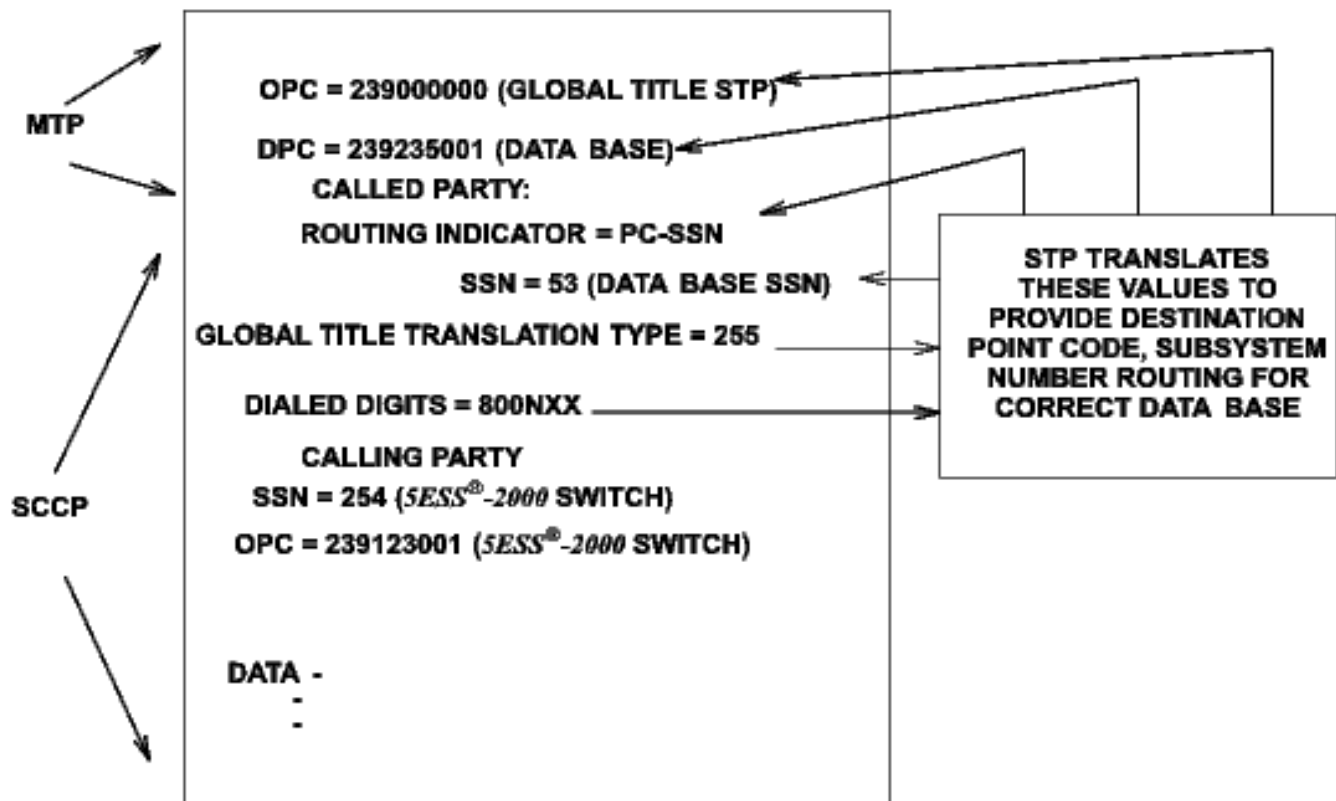


Figure 3.9-3 STP Message to Data Base (After Global Title Translation)

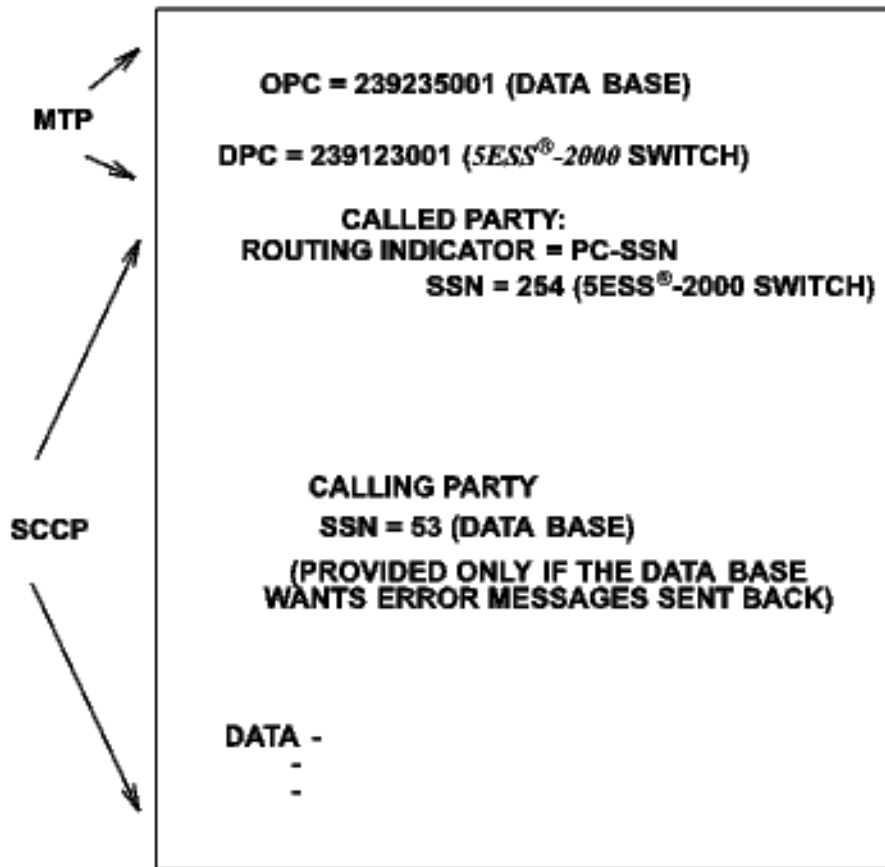


Figure 3.9-4 Data Base Reply Message

3.9.2.3 Capability Code (Alias Point Code)

An alternative to choosing a pair of STPs to do global title translations for features is to choose a Capability Code. A Capability Code is a single point code that is recognized by both of the global title STPs as being their point code.

The advantage of using Capability Codes instead of point codes of the STPs is that fewer messages are lost in the network when one of the mated STPs fails. If a Capability Code is not used, an STP failure will result in a few in-transit messages being lost. An additional advantage is that if the A-links to one of the global title STPs are lost, global title translations will be done at the mate rather than rerouting the messages over the C-links.

In a noncapability code routing configuration, the paired STPs perform the global title translations with half of the traffic sent to one STP and the other half to the other. In this configuration, if an A-link to one of the global title translation STPs (STP 0) goes down, all the messages sent from the end office switch travel over the A-link to the other STP (STP 1). Since half of the traffic still has the destination code of STP 0, the traffic bound for STP 0 travels over the A-link to STP 1 and the C-link between STP 1 and STP 0 (see Figure 3.9-5).

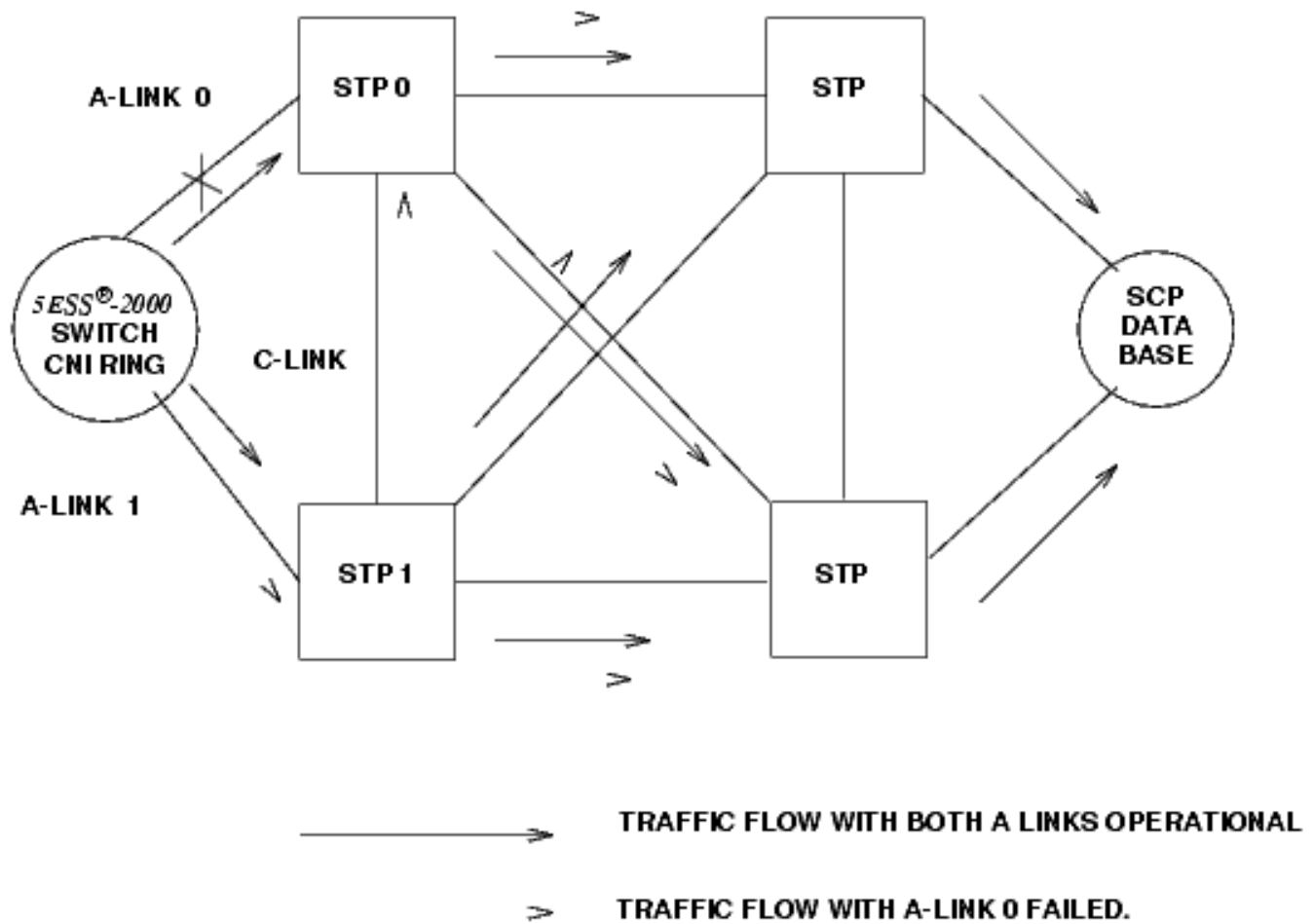


Figure 3.9-5 Noncapability Code Routing Configuration Noncapability code routing configuration

When capability codes are used, the global title translation traffic is routed equally across the A-links to the STP pair. If an A-link to STP 0 fails, all of the global title traffic goes to STP 1 for translation (see Figure 3.9-6).

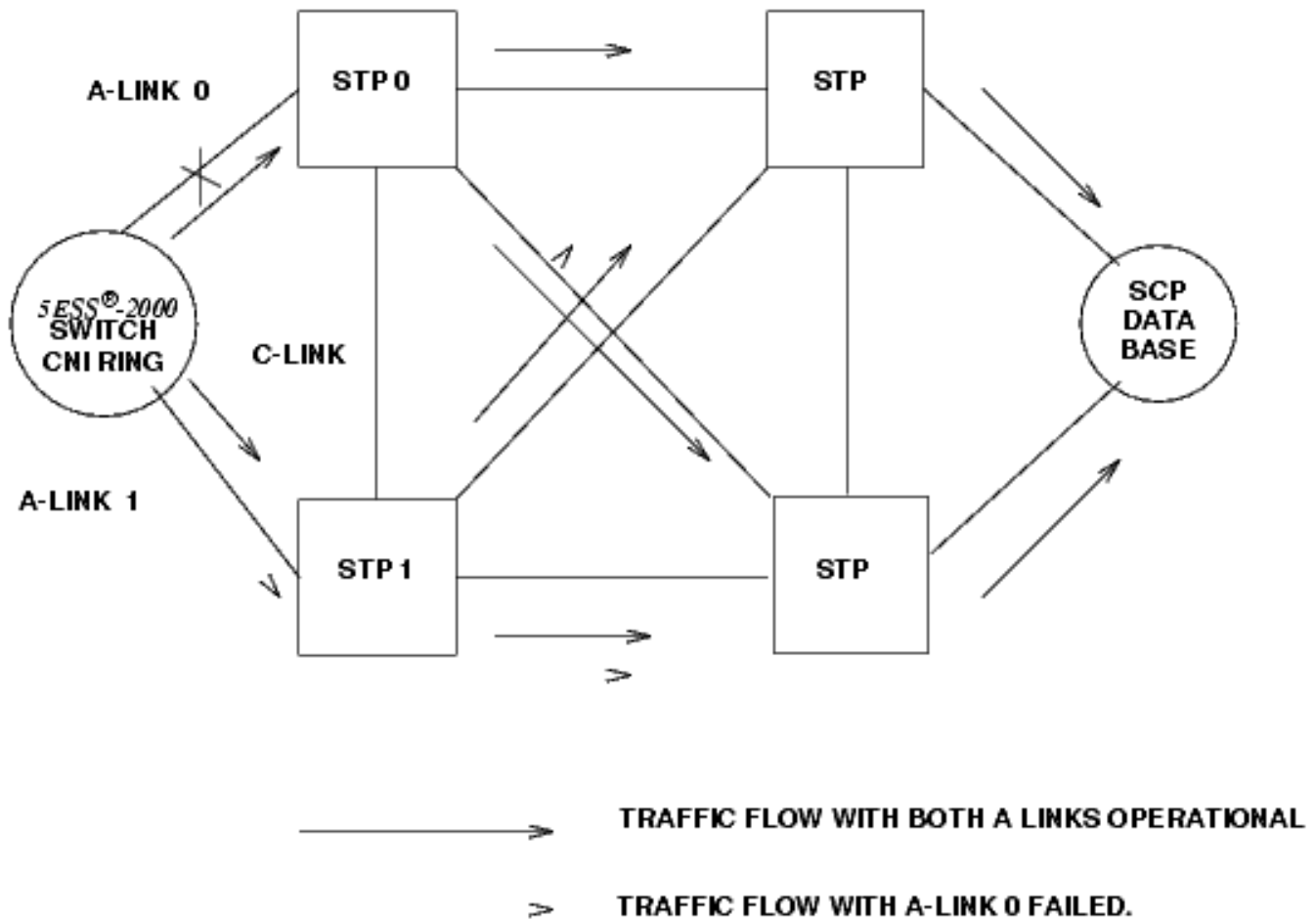


Figure 3.9-6 Capability Code Routing Configuration Capability code routing configuration

3.9.2.4 Linking the 5ESS®-2000 Switch to the CCS Network

In populating the CNI data base, the information needed for linking the switch to the CCS network is provided later. Shown in parentheses are the recent change views or files that depend on the information.

- Switch Point Code (Recent Change View 15.1)
- Point Code for one of the STPs in a pair (Recent Change Views 15.2 and 15.9)
 - Number of Signaling Links to this STP
 - Signaling Link Code (Recent Change View 15.2)
- Point Code for the other STP in a pair (Recent Change Views 15.2 and 15.9)
 - Number of signaling links to this STP
 - Signaling Link Code (Recent Change View 15.2).

3.9.2.5 SSP800 Service and LASS

The following information is required for populating the data base and recent change views for SSP800 service

feature and LASS.

- Global Title Translation Preferred STP Point Codes:
 - If Capability Code (Alias Point Code) routing is used:

Capability Code (Recent Change View 15.9, Network File, or 15.11, Global Title).
 - If the routing is not Capability Code Routing but global title translations are done at a remote STP pair.

Point Code of one of the Remote STPs (Recent Change View 15.9, Network File or 15.11).

Point Code of the other Remote STP (Recent Change View 15.9, Network file or 15.11).
- Global Title Translation Type for SSP800 and LASS in switch (Recent Change View 8.17)
- SSP800 Subsystem Number in switch (Recent Change Views 8.17 and 15.10)
- SSP800 Data Base Cluster(s) (Recent Change View 15.9).

3.9.2.6 ISUP Trunking

The Recent Change View 15.9 requires the identification of the ISUP trunking far-end office(s) cluster(s).

3.9.2.7 Office Dependent Data in the Direct Link Node

Up to this point, we have discussed the CNI data base population for SSP800 service and ISUP trunking features. There are other data base considerations for SS7 protocol services. Some of these are as follows:

- The switch office dependent data (ODD) in the direct link node (DLN) of the CNI ring.
 - It is necessary for the DLN to maintain a copy of several static administrative module (AM) office dependent data relations. The trunk signaling requires that the following relations be kept in the DLN.

LAB7_PCI: SS7 label to point code index relation

PCI_PRT: Point code index to port relation
 - LASS, LIDB, CAS and ICCV: Requires additional relationships to be kept in the DLN.
- The TCAP for SSP800, LASS, and LIDB service requires additional relations to be kept in the DLN.

When the DLN is initialized, the AM relations are read and transferred via the interprocessing message switch (IMS) direct memory access (DMA) channel to the DLN. Maintaining duplicate copies of the relations subsequent to initialization is accomplished by the use of trigger functions that notify the DLN of AM status relation changes.

3.9.3 Data Base Population

Following is the recent change sequence to consider when populating the CNI data base for new starting offices.

- (1) The CNI is installed or grown as covered in the Installation Handbook.

The temporary CNI-related data files are created based on user input gathered in response to a series of

office environment and hardware equipage related prompts. These prompts are generated by a script invoked at the RC/V terminal or Supplementary Trunk and Line Work Station (STLWS). This temporary data is used to facilitate installation of the CNI Ring without the need for any office specific data. Refer to the Installation Handbook for procedures to install temporary data files.

NOTE: The temporary data must be replaced with actual, complete, site-specific data prior to placing the ring in service.

(2) Populate Recent Change View 15.1 (Office Data).

(3) Populate Recent Change View 15.2 (Link Node Data). Enter a view for each signaling link node that is connected to the adjacent STP pair.

NOTE: The signaling link node must be out of service and the **major state** field must be set to **UNA** before the link information can be updated.

(4) Populate Recent Change View 15.3 (Logical to Physical). Populate a view for each signaling link that transmits CCIS6 trunk signaling messages over high (56 kb/s) or low speed links (4.8 kb/s).

(5) Populate Recent Change View 15.12 Network Routing Data when:

- The switch is routing SS7 messages to another network.
- GTTs are performed in an STP that is located in another network.
- An SCP that is used for SS7 based features is located in another network.
- A far-end office is located in another network (ISUP trunks, Recent Change View 5.1).
- A switch in another network is being sent TCAP messages for LASS.

(6) Populate Recent Change View 8.15 (CCS Office Parameters), if APSDN or NS800 is provided by the switch.

(7) Populate the Recent Change View 15.10 (Subsystem Numbers — subsystem number 3 is needed for ISUP flow control) when using SS7 based features for:

- NS800
- APSDN
- ASP
- LASS
- LIDB
- CCS7 trunking.

NOTE: The subsystem numbers must correspond with the network subsystem values, and the values assigned to the particular applications on Recent Change View 8.17.

(8) Populate Recent Change View 15.11 (Global Title Translation) when Global Title Translations are to be done using Capability Codes, or if translations are not to be done at the local STP pair.

If no entry is made in the 15.11, the Global Title Translations are performed at the local STP pair. The point codes are stored in the general translator, 256.

NOTE: The **translation type** must correspond with the value assigned to the applications on Recent Change View 8.17.

- (9) Populate Recent Change View 8.17 (Direct Signaling Application), if the subsystem numbers are assigned on Recent Change View 15.10.
- (10) Populate Recent Change View 15.9 (Cluster Routing Data) for:
 - Each local STP cluster.
 - Each far-end office cluster (ISUP trunks defined on Recent Change View 5.1).
 - Each STP where Global Title Translations are performed.
 - Each service control point (SCP) where routing information is stored for SS7 based features (that is, LIDB, NS800, APSDN, and ASP).
 - Each switch where LASS TCAP messages are sent.
- (11) Populate Recent Change View 15.18 when:
 - The local STP pair and connecting office reside within the switch's small network.
 - The local STP pair resides in another small network.
- (12) Recent Change Views 15.4 through 15.8 are initialized with an extensive set of standard input data. The existing report data should not be manipulated, but a customized measurement report may be created by entering the following views:
 - Define a new user view on Recent Change View 15.5.
 - If restrictions are needed on specific measurements, define an exception table on Recent Change View 15.6 for the user view defined on Recent Change View 15.5.
 - Schedule the report on Recent Change View 15.8 using one of the corresponding report types.

Refer to appropriate sections of 256-080-100, *Translation Guide*, for a detailed description of each view and possible field values that can be used to populate each field.

3.10 EXTENDED ACCESS AND ALTERNATE A-LINK (E/A LINK) ROUTING

3.10.1 Feature Description

The Extended Access Links and Alternate A-Link Set Routing (E-LINK) feature provides the switch in the local exchange carriers' (LEC) SS7 networks with the capability to connect the signaling links between signaling end points (SEP) and non-home signal transfer point (STPs). At the switch, Alternate A-link Set Routing is the use of E-links to provide alternate routing to traffic that is carried by A-links, and vice versa.

This feature is secured; that is, it cannot be used until a Right-To-Use (RTU) fee has been paid to Lucent Technologies.

3.10.2 Availability

These features are available with the 5E9(1) and later software releases.

3.10.3 Feature Environment

Figure 3.10-1 illustrates E-link and A-link routing.

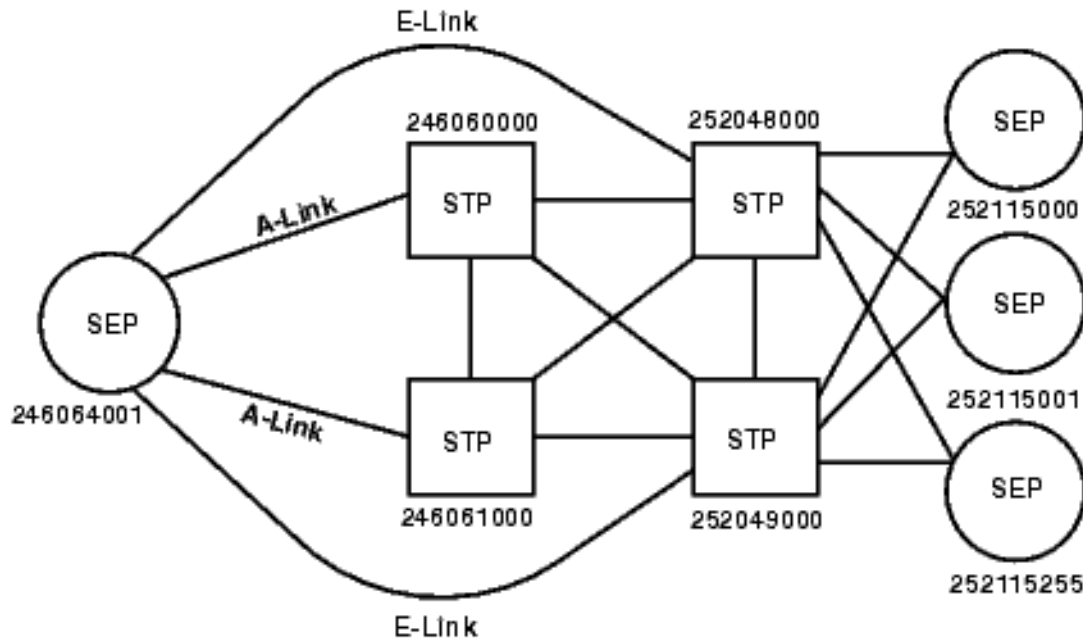


Figure 3.10-1 E-Link and A-Link Set Routing

With respect to signaling points, primary routes for destination points have the highest routing priority relative to all other provisioned routes used for the same destination point. Alternate routes are lower in routing priorities for the destination point relative to the route of highest priority (that is, primary route) used for the same destination point. A-links or E-links may be provisioned as primary or alternate routes for destination points.

The STPs that are connected to switches via links that are designated, via provisioning procedures, as type "A" are defined as PRIMARY or HOME STPs with respect to those switches. The STPs that are connected to switches via links that are designated as type "E" are known as OTHER STPs with respect to those switches. Hence, whether STPs are conceptually known as PRIMARY, HOME, or OTHER depends on how the links are designated. This concept is used throughout this section.

The following are E-link characteristics:

- An E-link is an SS7 signaling link that connects a switching office and an OTHER STP.
- E-links are installed as a pair and provisioned as a combined link set from a switch to any OTHER STP pair.

The E/A-Link feature provides the following capabilities between a signaling end point (that is, switching office) and an OTHER STP:

- E-link connection between switches and OTHER STP pairs.
- At SEPs, use A-link sets as backup under certain conditions (that is, A-link set serves as the alternate route) - this is also known as alternate access.
- At SEPs, provide alternate routes for intralocal and interlocal cluster routing.
- At SEPs, use E-link sets as backup under certain conditions (that is, E-links serve as the alternate route for A-links).
- Provide routing of SS7 messages over E-links.
- Provisioning of E-links only as backup routes; in this case, the links would remain in the active state without being used as the primary route for any destination point. It is recommended that E-links be used in an SEP as both the primary and alternate route.
- At SEPs, provide simultaneous support of routing over A-links and E-links for different destinations.

The previously listed capabilities are provided without the need for SEPs to be identified with multiple or alias point codes.

3.10.4 Background

Motivations for implementing the E/A-Link feature in the LEC's network are as follows:

- Improve survivability - E-links provide additional routes to destinations to further minimize SEP isolation. The E-link sets serve as alternate routes in the event of failed A-link sets. Also, A-link sets serve as alternate routes in the event of failed E-link sets.
- Direct message routing - E-links may be used to allow traffic to be directly routed to OTHER STP pairs or quads from SEPs in order to use fewer intermediate STPs. This speeds up call processing, and thereby, improves network performance.

3.10.5 Recent Change And Verify

Table 3.10-1 shows the Recent Change fields that are impacted by the E-link feature. Refer to 235-118-2xx, *Recent Change Reference* for a detailed description of each view and possible field values that can be used to populate each field.

Table 3.10-1 Recent Change Views Impacted By E-LINK

VIEW NUMBER AND FIELD NAME	DESCRIPTION
15.1 LOW PRI SRST	The timer for the Signaling Route Set Test (SRST) message transmission interval for routes that are alternate or lower priority (not current) route.
15.2 LINK TYPE	The type of link used for signaling between a 5ESS®-2000 switch and a signaling point.
15.9 ROUTING FLAG	The network routing flag is used to determine the level of routing to be performed.
15.9 PRI ROUTE	The linkset number for primary route based on the routing level.

15.9 ALT1 ROUTE	The linkset number for alternate 1 route based on the routing level.
15.9 ALT2 ROUTE	The linkset number for alternate 2 route based on the routing level.
15.12 ROUTING FLAG	The cluster routing flag is used to determine the level of routing to be performed.
15.12 PRI ROUTE	The linkset number for primary route based on the routing level.
15.12 ALT1 ROUTE	The linkset number for alternate 1 route based on the routing level.
15.12 ALT2 ROUTE	The linkset number for alternate 2 route based on the routing level.
15.18 NID	The network identifier of a point code to where CCS messages are routed.
15.18 CLUSTER	The cluster number of a point code to where CCS messages are routed.
15.18 MEMBER	The member number of a point code to where CCS messages are routed.
15.18 ROUTING FLAG	The member routing flag is used to determine the level of routing to be performed.
15.18 PRI ROUTE	The linkset number for primary route based on the routing level.
15.18 ALT1 ROUTE	The linkset number for alternate 1 route based on the routing level.
15.18 ALT2 ROUTE	The linkset number for alternate 2 route based on the routing level.
15.18 LAST MEMBER	The last member number in the range of members to be inserted.

3.10.6 Signaling Indicators

The current signaling indicators, TSIG, DSIG, and TCAP have three states: ACT, OOS, and UNEQ. However, signaling can be affected by congestion in the links or the direct link node (DLN). When this occurs, messages may be returned/dropped.

NOTE: TCAP messages can have a return bit so when problems occur and the message cannot be delivered, it is returned to the sender.

For this reason, a new state of degraded (DGR) is added to these indicators to show that not all messages may make it to their destination.

Two other changes affect TCAP functionality. The first change, which affects DSIG as well, is that signaling link congestion will no longer be a condition for turning off TCAP and DSIG capabilities. Earlier switch releases turned off these capabilities in an attempt to complete the more important TSIG messages. Operator Services Position System (OSPS) offices, however, mostly use TCAP and/or DSIG services.

Secondly, the TCAP indicator is also now affected on a subsystem basis. Under the current design, the TCAP capability is turned off if the default point codes (PCs) in the global title table are inaccessible. Other PCs for different global title translations may still be functioning and able to handle traffic. The new design bases TCAP usability according to each subsystems global title STP pair accessibility. This will keep TCAP up in either an active or degraded state as long as one global title PC is accessible.

3.10.7 Point Codes Out-Of-Service

Currently, the switch prints an ROP output message when a DPC becomes accessible or inaccessible. This information is also available with the command `OP:C7NET`. To have faster access to this information, inaccessible DPCs are displayed on the CNI 118 page.

3.10.8 Feature Interactions

This feature in and of itself is independent of any other feature. However, under certain network configurations, the E-link feature may be dependent on the Full Point Code Routing (FPCR) feature. For example, if, when the E-link feature is added to a signaling end point (SEP) and, at the same time, a reorganization of LATA point code assignments is taking place, FPCR is required in order to allow for a more efficient transition and maintenance of network reliability. If the E-link is being added to a SEP and no LATA reorganization is taking place, then FPCR is not required with the E-link feature.

3.11 SS7 F-LINKS

3.11.1 Feature Description

The SS7 F-Links feature (99-CP-3627) provides a direct signaling connection between signaling end points (SEPs). This is illustrated in Figure 3.11-1.

Prior to this feature, SEPs (that is, switches or databases) communicated to their home signal transfer point (STP) pair through A-links, or to a remote STP pair through E-links. Direct links between SEPs were not supported.

SS7 F-Links is a secured feature (SFID=274) and a right-to-use (RTU) fee must be paid to Lucent Technologies before enabling information is provided.

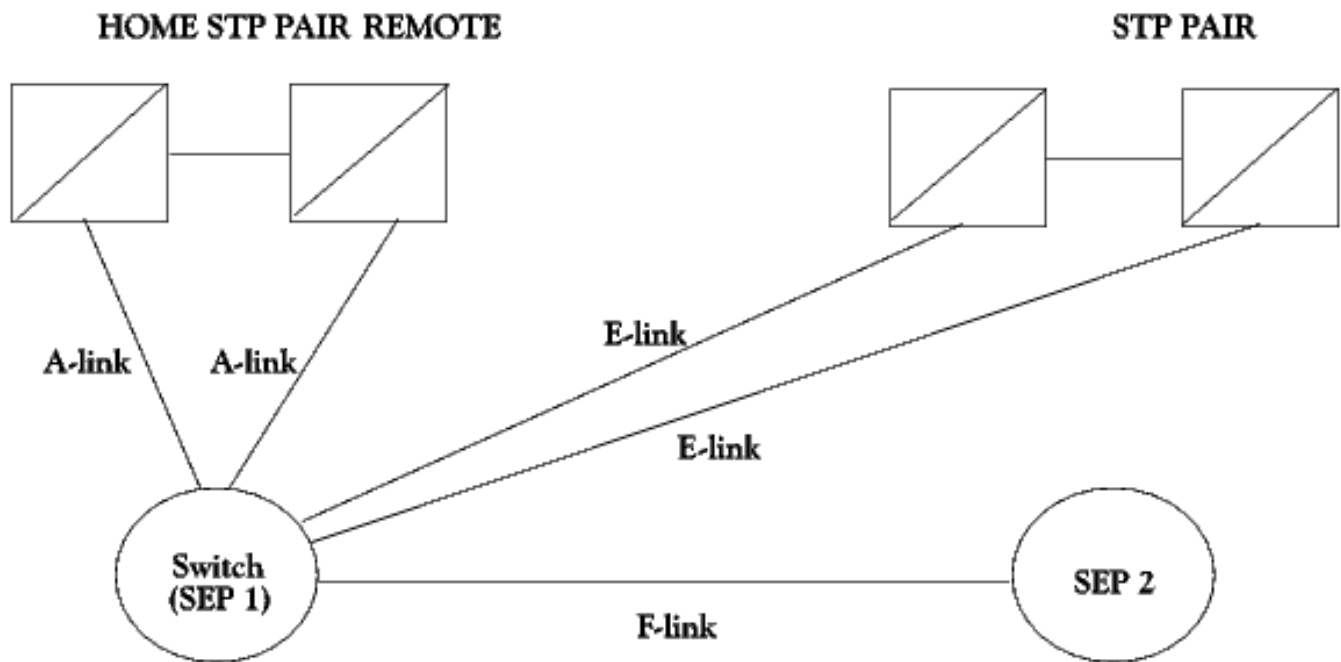


Figure 3.11-1 SS7 Signaling Connections

3.11.2 Availability

This feature is available as a software update to the 5E12 software release.

3.11.3 Feature Environment

This feature is provided on a per-switch basis.

3.11.4 Cross References

The following cross references apply to this feature:

- SS7 F-Links, feature number 99-CP-3627.

3.11.5 Background

Not applicable.

3.11.6 Feature Operation

Signaling operates the same for F-links as for A-links and E-links. This includes:

- Strategies for alternate routing
- Signaling link management
- Congestion control capabilities
- Signaling route management
- Changeover procedures, which are invoked when:
 - One link of an F-linkset fails, is blocked, or inhibited. Changeover is performed to another in-service link in the linkset.
 - An F-linkset fails. Changeover is performed to the next available alternate route as provisioned.
- Changeback procedures, which are invoked when at least one link of an F-linkset is restored, unblocked, or uninhibited. Changeback is performed to the reactivated link(s) in the linkset.

3.11.7 User Operation

The service provider must unlock this secured feature and assign F-links using recent change procedures.

3.11.8 Engineering

3.11.8.1 Hardware Resources

The physical hardware used for terminating an F-link is the same supported common network interface (CNI) link interface (LI) and link node (LN) hardware used for A-link or E-link signaling link terminations.

3.11.8.2 Software Resources

No software considerations are associated with this feature.

3.11.8.3 Transition Considerations

No transition considerations are associated with this feature.

3.11.9 Interactions and Limitations

No interactions or limitations are associated with this feature.

3.11.10 Incompatibilities

No incompatibilities are associated with this feature.

3.11.11 Dependencies

Before an F-linkset can be provisioned as an alternate signaling route for a destination point code, the E-Link Access and Alternate A-Link Set feature (SFID=131) must be activated.

3.11.12 Isolation Constraints

No isolation constraints are associated with this feature.

3.11.13 Recent Change Provisioning

The service provider must unlock and activate this secured feature by populating Recent Change view 8.22, *Secured Feature Upgrade*:

FIELD	* VALUES
FEATURE ID	274
MODULE	(Office or SM 1-192)
PASSWD	(Provided by Lucent Technologies SFID Administrator)
ACTIVE	Y
	"Y" - Turns on (unlocks) the feature
	"N" - Turns off (locks) the feature

Recent change views impacted by the SS7 F-Links feature are listed in Table 3.11-1 .

Table 3.11-1 Recent Change Views Impacted By F-Link

VIEW NUMBER AND FIELD NAME	DESCRIPTION
15.2 LINK TYPE	The type of link used for signaling between a 5ESS®-2000 switch and a signaling point.
15.9 PRI ROUTE	The linkset number for primary route based on the routing level.
15.9 ALT1 ROUTE	The linkset number for alternate 1 route based on the routing level.
15.9 ALT2 ROUTE	The linkset number for alternate 2 route based on the routing level.
15.18 PRI ROUTE	The linkset number for primary route based on the routing level.
15.18 ALT1 ROUTE	The linkset number for alternate 1 route based on the routing level.
15.18 ALT2 ROUTE	The linkset number for alternate 2 route based on the routing level.

* See 235-118-2xx, *Recent Change Reference* for detailed information on allowed values.

3.11.14 Customer Premises Equipment (CPE)

Not applicable.

3.11.15 Maintenance Considerations

Maintenance capabilities and strategies currently in place for A-links or E-links also apply to F-links. This includes:

- Manual maintenance capabilities, or manual controls and test capabilities executed through input messages or display pages
- Automatic trouble detection, isolation, recovery actions, and reporting.

3.11.16 Administration

3.11.16.1 Measurements

Signaling link and linkset measurements that are presently collected for A-links and E-links are also collected for F-links. Refer to 235-070-100, *Administration and Engineering Guidelines* for descriptions of these measurements.

3.11.16.2 Billing

This feature does not impact billing.

3.12 FULL POINT CODE ROUTING (FPCR)

3.12.1 Definition

The Full Point Code Routing (FPCR) feature provides the switch in the local exchange carriers' (LEC) networks with the capability to directly route traffic on specific combined link sets to other STP pairs based upon the 24 bits of the Destination Point Code (DPC). This makes for a more efficient network.

This feature is secured; that is, it cannot be used until a Right-To-Use (RTU) fee has been paid to Lucent Technologies.

3.12.2 Availability

This feature is available with the 5E9(1) and later software releases.

3.12.3 Feature Description

The Full Point Code Routing (FPCR) feature allows switches in the LEC networks to force traffic to directly route on specific combined link sets to other STP pairs. This is accomplished by routing SS7 signaling messages based upon the 24 bits of the DPC.

This capability may be employed when a specific dedicated combined link set is legally designated as the sole route that may be used out of the switch. Backup to alternate combined link sets is possible and provided. This feature opens up FPCR at the switch, and is supported by combined link sets. The FPCR is allowed over combined link sets and direct link sets. Direct link sets may or may not be part of a combined link set. Also, link sets may or may not be internetwork link sets. With respect to a switch at a time, all members of a cluster (CLU) must be routed to by using FPCR when routing to at least one member of the cluster via FPCR.

For clusters, whose members are routed to using FPCR, the following applies:

- When a Transfer Cluster Restricted (TCR) is received at the switch, all members of the cluster are marked as "restricted" over the affected route.
- When a Transfer Cluster Prohibited (TCP) is received at the switch, all members of the cluster are marked as "prohibited" over the affected route.
- When a Transfer Cluster Allowed (TCA) is received at the switch, all members of the cluster are marked as "allowed" over the affected route.

A cluster may be changed from a non-FPCR cluster to an FPCR cluster, and, similarly, from an FPCR cluster to a non-FPCR cluster with the signaling link(s), signaling route(s), and signaling point in any state.

Routing data may be updated while the signaling link, signaling route, and signaling point status for the route(s) to be updated is "available." This allows deployment of the full point code routing feature in the switches without service disruption.

3.12.4 Background

The motivation for implementing the FPCR feature in the LECs' switching offices is to improve network performance by allowing force traffic to be directly routed to more efficient and less problematic routes.

3.12.5 User Perspectives

An FPCR cluster refers to a cluster where all members of the cluster are routed to using the full point code routing.

If a message is routed to a member that has not been added by Recent Change, then there is no routing data for the member and the message cannot be routed.

Cluster routing refers to a cluster where routing is done at the cluster level if there is no routing data for a member. If a message is routed to a member that has not been added by Recent Change, then the message is routed using the routing data at the cluster level.

NOTE: All the FPCR members should be added before changing from cluster level routing to FPCR. Otherwise, messages routed to those members not added will NOT be delivered.

The recent change procedure sequences for changing routing data from cluster routing to full point code routing (member routing) are as follows: (Assume that routing data has existed for cluster level routing.)

- Populate Recent Change View 15.18 (Member Routing Data). Enter routing data to all the FPCR members.
- Modify Recent Change View 15.9 (Cluster Routing Data). Assign zero to the PRI ROUTE field after all the FPCR members of the cluster have been added. At present, the cluster is an FPCR cluster. All the members of the cluster are routed to using the full point code routing. Messages are NOT routed to those members not added.

3.12.5.1 Recent Change and Verify

Table 3.12-1 shows the Recent Change fields that are impacted by the FPCR feature. Refer to 235-080-100, *Translation Guide* for a detailed description of each view and possible field values that can be used to populate each field.

Table 3.12-1 Recent Change Views Impacted By FPCR

VIEW NUMBER AND FIELD NAME	DESCRIPTION
15.18 NID	The network identifier of a point code to where CCS messages are routed.
15.18 CLUSTER	The cluster number of a point to where CCS messages are routed.
15.18 MEMBER	The member number of a point code to where CCS messages are routed.
15.18 ROUTING FLAG	The member routing flag is used to determine the level of routing to be performed.
15.18 PRI ROUTE	The linkset number for primary route based on the routing level.
15.18 ALT1 ROUTE	The linkset number for alternate 1 route based on the routing level.
15.18 ALT2 ROUTE	The linkset number for alternate 2 route based on the routing level.
15.18 LAST MEMBER	The last member number in the range of members to be inserted.

3.13 OPERATIONS, ADMINISTRATION, AND MAINTENANCE

This section describes the SS7 measurements and reports available to the user. The section is broken down into two parts.

- **Measurement Descriptions:** This part describes the measurements taken and the occurrence that those measurements record. It also describes the source of the measurements.
- **Report Descriptions:** The scheduled and demand reports are described with some examples of the report output.

Measurement Descriptions

A measurement is a "register" that represents the cumulative total of, or the duration of, some occurrence. A measurement may be an action that occurred within the office as a response to some occurrence outside the office. Some of the measurements pertain to the common network interface (CNI) office and others pertain to the entire common channel signaling (CCS) network. Many of the measurement timers are generally stored in units of milliseconds (some exceptions are noted in the description of the particular measurements). Most measurements register in the node processor or link interface circuits. Some measurements are of occurrences identified by the central processor.

The measurement data organized within the main memory disk files is generated from the measurements collected in the node processor, link interface and central processor. To access the data requires some identification scheme. The measurements are named using the following convention:

- The mnemonic derived from a set of abbreviations representing a typical occurrence in a CNI-equipped office, represents as closely as possible the occurrence being measured.
- The suffix T signifies a measurement of an interval, not the number of occurrences.
- The suffix TE signifies a threshold has been exceeded.
- Names include only letters and digits (no special characters).
- Names are unique and contain no more than 12 characters.

The measurement names are used by the measurement output control table used to control measurements for operation, administration, and maintenance.

3.13.1 CNI Measurement Reports

3.13.1.1 Report Types

There are two types of CNI measurement reports: fixed and flexible. The fixed reports cannot be modified by the user. The fixed reports are as follows:

SNPR1:	Signaling Network Performance Report, Part 1
SNPR2:	Signaling Network Performance Report, Part 2
SEPR:	Signaling Equipment Performance Report
MPR:	Machine Performance Report
30LMPR:	30-Minute Marginal Performance Report
RINGEX:	Ring Peripheral Controller Overflow Report.

The flexible reports are as follows:

NFDISK:	Regular Disk Report (prints out all values)
NFDISKEX:	Exception Disk Report (prints only where thresholds are exceeded)
NFLPM:	Regular Last Period Measurement (prints all values)
NFLPMEX:	Exception Last Period Measurements (prints only where thresholds are exceeded).
ZMMPR:	Signaling link 15-Minute Machine Resource Performance Report.

More detailed information on the previous listed reports can be found in the 235-070-100, *Traffic and Plant Measurements Manual, Appendix 1*.

3.13.1.2 Source of Measurements

3.13.1.2.1 Plant and CNI Measurements

The two basic sources of measurements in an office are as follows:

- (1) **Plant Measurements** - These measurements originate in the *UNIX*[®] system real-time reliable (RTR) and are not discussed in the document. These measurements are covered in 235-070-100, *Traffic and Plant Measurements Manual, Appendix 1*.
- (2) **CNI Measurements** - These are occurrences recognized by the CNI-equipped office.

The CNI measurements are classified as ring node oriented, link oriented, and total office oriented. This distinction is useful from a maintenance standpoint since faults generally occur in these categories.

The measurement data is collected, stored, and distributed to various destinations within and outside the office. The CNI reports and plant measurement reports appear on the maintenance terminal and printer. Support organizations can request plant or CNI measurement data.

3.13.1.2.2 Ring Node Oriented Measurements

Ring node oriented measurements include ring blockages, node isolations, and ring read/write errors. Ring node measurements are mostly concerned with counts and transmission errors relating to internal messages (such as, messages between the central processor and the ring). Software in the node either pegs the counts or notifies the central processor. The counts are maintained in buffers in the node processors (and possibly in the central processor). Occasionally, an error notification is sent to the central processor to report error conditions in the ring. In addition to responding to the reported error, software in the central processor often updates the corresponding per-office counts and/or per-node counts. This report to the central processor occurs in real time independently from the periodic data collection. The measurements maintained in the central processor are collected for history file generation at the same time the node counts are collected.

The node also collects the link counts maintained by the link interface. The link interface counts are read by the node processor and placed in the buffers for subsequent reporting to the central processor.

The interprocess message switch (IMS) measurement descriptions identify three types of ring node oriented measurements as follows:

- (1) RPC - Per-node measurement originated in a ring peripheral controller
- (2) IUN - Per-node measurement originated in some ring node other than a ring peripheral controller
- (3) NP - Per-node measurement originated in any node processor.

3.13.1.2.3 Link Oriented Measurements

Link oriented measurements contain traffic volume counts and error conditions related to CCS messages. Some examples are as follows:

- Signaling errors
- Link failures
- Link congestions
- Buffer overloads.

The counts reflect the operating load of the system. This data is most useful in engineering the office and the entire CCS network. This category of measurements also reflect network abnormalities; such as, processor outages and emergency restarts.

The link oriented measurements are maintained in buffers in the link interface circuits and the node processors (and possibly in the central processor when notified by the node). The link interface circuit allows messages to enter and exit the CNI system. Since the link interface is a buffer circuit between the node and the data link, the counts pegged by the link interface are related to specific traffic counts. The measurements are usually taken from a circuit standpoint rather than on a message basis.

Other link-related counts, pegged by the node software, are based on the message discrimination performed by the node. Since the node software has a view of the node's function, it can recognize larger events than the link interface. These counts are maintained in the node.

3.13.1.2.4 Total Office Measurements

The total office measurements reflect the view of various occurrences in an office. Some of these indicate the

impact of corresponding per-link and per-node occurrences on the entire office. Others are not specific to any link or node and are, therefore, inherently total office counts. The office measurements include processor outages, initializations, ring failures, link failures, and various counts related to message processing in general (not specific to any link or node). These counts are maintained solely in the central processor. The measurements are pegged in the central processor and are either recognized by it or reported to it by the nodes when they occur.

The IMS measurement descriptions identify the following two types of total office measurements:

- (1) **Office** - These are total office measurements.
- (2) **CHN** - These are measurements oriented for a particular channel (possibly in a ring node or the central processor). When a message is to be read from or written to the ring, an association is made between the open channel and the buffer containing the message by the use of a queue that is dedicated to the channel. The central processor manages the 256 possible channels (each intended for a specific type of message) that can carry messages.

3.13.1.3 Measurement Process Phases

The measurement history files are used to store the transient data associated with measurements. The data is considered transient since no cumulative day-to-day record is automatically generated. The generation of measurement history data involves three phases as follows:

- (1) **Data Generation** - Recognizes and pegs the counts in software.
- (2) **Data Collection** - Periodically accumulates the raw measurements from all nodes.
- (3) **Data Processing** - Creates history files via the measurement output control table.

These phases take the raw measurement values from the buffers in the various processors (node processors and the central processor), cumulate them, and organize them into user accessible data files.

To be measured, an occurrence must first be recognized by the application. This takes place in the various processors in real time. The link interface maintains counts of CCS level 2 protocol measurements for its associated links. The counts represent link related measurements. The cumulative counts are copied to buffers in the node processor of each ring node at data collection time. Likewise, the node processor maintains counts of various occurrences related to messages and the ring. These are stored in buffers in the node processor. Every 5 minutes, the control processor broadcasts a message to all ring nodes requesting the measurement data in the ring node buffers. As each ring node receives this message, the data in the buffers is sent to the control processor to be stored in main memory.

NOTE: If IMS measurements are not inhibited, all nodes respond to the message. If IMS measurements are inhibited, only the ring peripheral controller nodes respond. The counts in the central processor measurement buffer (except inhibited measurements) are then combined with the counts from the ring nodes to form a complete set of measurement data.

The central processor, ring node, and link interface buffers are cleared every 5 minutes and begin to accumulate data for the next 5-minute period. The collected data resides in the main memory.

The data collected by the central processor every 5 minutes consists of IMS, CNI, and application measurement counts. The 5-minute measurement collection is the smallest collection period available to the measurement output control table and the user. All subsequent data processing builds on the data set. If IMS measurements are inhibited, some of the IMS counts are not accumulated any further by the central processor. The following are three limitations that should be kept in mind when analyzing measurement data:

- (1) Although the measurements register in real time, the report generation software becomes aware of them only at 5-minute intervals. For reporting purposes, an element of measurement data can be up to 5 minutes old.
- (2) If just one ring node is faulty or out of communication with the ring (for example, the node processor fails), the measurement data for an affected 5-minute interval is incomplete. That ring node is not reporting any measurements. Data from all ring nodes must be combined in main memory when building the measurement data. The problem is relieved by invalid or incomplete data being flagged on output reports.
- (3) If IMS measurements are inhibited, some reports may display IMS counts as zero. Flexible format reports with IMS measurements either ignore these counts or they are not output at all. Also, the `DUMP:SMEAS` command refuses requests to display certain IMS counts. Counts that are unavailable when IMS measurements are inhibited include the following:
 - All IMS counts collected from IMS user nodes
 - All IMS channel measurements
 - All IUN counts other than **IMNPDIF**, **OOSCFG**, **OOSCFGT**, **OOSAU**, **OOSAUT**, **OOSMN**, and **OOSMNT**.

The final phase in generating the data files is the processing of the data residing in the main memory. This processing is intended to generate files of measurement data that are useful in producing reports and cover longer periods of time. The basic data file used is the last 15-minute file. To get this file, the 5-minute measurements are cumulated in the main memory for 15 minutes. Every 15 minutes, the cumulated data is written to disk as the **L15M** file. The focal point of the data base processing is the history file descriptor table which is one of the output control tables. Every 15 minutes, it is scanned for processing measurement data. Any processing that needs to be done is specified in the history file descriptor table. This allows users to specify measurement collection periods that suit their needs. Upon completion of a history file, the report schedule table is scanned to generate any report necessary. The latest 5-minute measurement data is available for use in reports, but is not available for generating history files.

The data files used in the history file descriptor table consists of "current" measurements and "past" measurements. These files are collectively referred to as history files. The current measurement data files contain the cumulative totals for the current collection period. This data is copied into the corresponding past measurement file at the end of the current collection period. The past measurement files contain the measurement data for the entire preceding collection period, while the current measurement files at any given time may not contain data for the full collection period. Any history data files created are stored on disk and are available for reports. Each history file, however, is associated with a particular collection period; such as, "15 min," "1 hr," or "1 day." They are not associated with a particular day or time of day. In other words, the files are reused at the end of their respective collection periods. These files are not automatically backed up, and only certain measurement files are used in fixed reports.

3.13.1.4 Measurement Descriptions

Table 3.13.1-1 contains a list of the IMS measurements and their descriptions. Table 3.13.1-2 contains the SS7 CNI measurements and descriptions. The tables provide the measurement name, type, and description. The measurement type identifies the measurement specifically for some protocol, some particular unit, or the whole office. The measurement names and descriptions are presented alphabetically. They are intended to aid the reader in understanding the source, meaning, and use of each measurement. The descriptions are to help the user to develop their own views of the measurement data to schedule output reports using the measurement output control table.

The measurement descriptions reference other applicable measurements. These references may provide additional information and eliminate duplicate descriptions. When applicable, differences are noted. Unless otherwise indicated, transmit and receive measurements count the same thing only in opposite directions. For example, the signal units received measurement includes the same type of signal units as the transmitted measurement. This similarity also applies to the measurements of events related to one of the dual rings. The measurement definitions for ring 0 format errors are the same as ring 1 format error definitions.

Table 3.13.1-1 IMS Measurement Descriptions

NAME (TYPE)	DESCRIPTION
ABOFL (Office)	Long message type application buffer overflow. This count is for the long type single message read buffers referred to in ABOFS description. It is pegged when there are no more buffers of this type available.
ABOFS	Short message type application buffer overflow. Messages delivered to IMS channels in the single message read mode are copied into buffers allocated from a common pool. A pointer to the buffer is placed in the read list for the channel (see RBOF description). For memory efficiency, there are two buffer sizes, short and long. This count is pegged whenever an attempt is made to allocate a short type single message read buffer when the buffer pool is empty. If possible, the message is returned to its origination; otherwise, it is discarded.
ARRATT (NP)	Automatic ring recovery restoration attempts. If a node is alleged to be faulty, automatic ring recovery diagnoses the node by attempting a conditional restore. An isolated segment may contain nodes with no faults due to multiple failures on the ring. These are restored unconditionally when they become reachable by the automatic ring recovery after one of the faulty nodes are recovered. This count is pegged each time automatic ring recovery attempts to restore a node.
ARREXR (NP)	Automatic ring recovery restoration failure due to excessive restore rate. Each time the automatic ring recovery restores a node, it increments a counter in the equipment configuration data in addition to the ARRATT measurement. If the counter exceeds a certain threshold within a given time, the node has a recurring fault. This count is then pegged and the node is marked for manual intervention.
ARRFLR (NP)	Automatic ring recovery restoration failures. If the automatic ring recovery is unsuccessful at restoring a node, this count is pegged. If the failure to restore is due to a legitimate diagnostic failure, the node is marked for manual intervention. If the diagnostic is aborted due to other reasons, it is retried later. (See ARRATT description.)
BLK0 (Office)	Ring 0 blockage. This count is pegged once if a blockage is reported on ring 0 by one or more nodes during a particular interval (see the BLKG0 description). It is the cumulative count of incidents on ring 0 that result in blockages and a corresponding ring reconfiguration. Each incident may involve multiple blockage reports from several nodes.
BLK1 (Office)	Ring 1 blockage. See BLKG0 description.
BLKG0 (NP)	Ring 0 blockage. Each node contains a ring interface circuit used to access the dual rings. The circuit contains a buffer called a ring access circuit. Blockages are detected when a ring access circuit has been unable to propagate data to its downstream neighbor for a predetermined period of time. If too much time elapses without any data being transferred, a blockage is reported to the central processor and this count pegs for the reporting node. The node then dequeues some data to reset the blockage timers of upstream nodes. This is sometimes ineffective, resulting in multinode blockage reports.
BLKG1 (NP)	Ring 1 blockage. See BLKG0 description.
BUFSW (NP)	Ring receive buffer switch. When the node reads messages from the ring, the data is sent by direct memory access to buffers in the node processor memory. Each buffer has a fixed length. If the direct memory access data requires another buffer, it is interrupted, a new buffer is allocated, this count is pegged, and the direct memory access data continues.
CONFG (NP)	Begin/end point of isolation segment. This count is incremented whenever the specified node is either a begin isolation (BISO) or an end isolation (EISO) node. Whenever a node adjacent to this node is isolated, the node may become the begin or end point depending on how the ring is reconfigured (refer to SRNIAU or MRNIAU description). The begin/end node is not isolated. Rather, the ring interface circuits in the node cause ring 0 and 1 to loop on each other.

CONFGT (NP)	Duration of begin/end point of isolation segment. The length of time a node is either a BISO or EISO node.
CUTOUMSG (Office)	3B20D computer to 3B20D computer IMS messages. This is a cumulative count of all messages delivered between two channels in the central processor.
CUTOCUWDS (Office)	3B20D computer to 3B20D computer IMS message words. This is a cumulative count of all words delivered between two channels in the central processor. It is incremented by the size of a message when the message is queued for the destination channel.
CUTORMSG (RPC)	3B20D computer to ring peripheral controller IMS messages. This is a cumulative count of all messages transmitted to a specific ring peripheral controller. The ring peripheral controller may or may not be the final destination of the message. Messages queued in the write buffers are delivered to the ring at each invocation of the message switch.
CUTORWDS (RPC)	3B20D computer to ring peripheral controller IMS message words. This is the cumulative count of the size of all the messages transmitted to a specific ring peripheral controller. The count is in 3B20D computer words (each word is 4 bytes). (See also CUTORMSG description.)
DMAFLT (RPC/DLN)	Direct memory access fault. The central processor communicates with the node via both the direct memory access and program input/output requests. The direct memory access is used when large amounts of data needs to be sent to or from the ring and it is not necessary for the sending process to wait for completion. Hardware detects the fault (such as, incorrect address) when direct memory access data is being transmitted. When a fault is detected, the transmission via direct memory access is interrupted and this error is reported to the central processor, and the count is pegged.
DMAMISS (RPC)	Direct memory access missed. When the message switch wants to send messages to the RPC or DLN, it first checks to see if the RPC or DLN is ready to accept more messages (for example, is it finished with the direct memory access message sent by the last switch cycle). If the RPC or DLN is not receiving messages and is ready to receive, they can be used by the message switch to send messages to the ring. If the RPC or DLN are busy and cannot be used, this count pegs.
IDLE (NP)	A relative measure of node processor idle time. Tasks in a node (both message and maintenance processing) are scheduled by preemptive priority. When all other tasks have completed, the node processor executes the idle routine (this routine is assigned the lowest possible priority). This count is incremented by the idle routine in an amount proportional to the time spent idle. This idle routine also sets the idle flag indicating there is no work. The idle flag is checked and cleared every 10 ms by the overload monitor.
IFBPTER0 (NP)	Interframe buffer parity error on ring 0. The interframe buffer is considered to be part of the input circuitry of the downstream node. Parity errors detected in the interframe buffer is reported by the node. The error can be considered equivalent to a hard parity error, but occurring in the associated interframe buffer (see the RIPTER0 description).
IFBPTER1 (NP)	Interframe buffer parity error on ring 1. Refer to IFBPTER0 description.
ILLEGAL (NP)	Number of messages processed by the illegal message handler. This includes such messages as source match, destination channel closed, or returned messages. Refer to RTMSGSRC, MTINTCH, and MRRING descriptions.
IMNPDIF (NP)	Node processor data integrity flag. If this count is zero, the data collected is good. A count other than zero indicates the data collected by the central processor is incomplete. The following describes the meaning of the bits. The IMOFFDIF measurement describes how these bits are derived. In the following, the measurement value is 00000000abcd0efg0000000000000000h in binary: (a) Data collection period skipped (b) Data collection period aborted (c) Node did not respond (no measurements received) (d) Periodic data collection initialized (e) Data collection process faulted during data collection

	(f) Node removed (g) Node grown (h) Node initialized (this value is collected in the node).
IMOFFDIF (Office)	Per office data integrity flag. If this count is zero, the data collected is good. A count other than zero indicates that the data collected by the central processor is incomplete. The data integrity flag is used to determine if an event has occurred in the period of interest which causes the data collected for that period to be suspect. The data integrity flag is actually a decimal representation of one 32-bit word describing the error condition. To determine the meaning of the count, convert the representation of the 32-bit word from decimal to binary and analyze the bits. In the following, the measurement value is represented as 00000000ab0c0d0000000000000000000 in binary. Each bit in the word that is set (more than one can be set) indicates a particular error: (a) Data collection period skipped (b) Data collection period aborted (c) Periodic data collection initialized (d) Data collection process sustained a fault.
INBOF (NP)	Failure to obtain a new ring receive buffer. Messages are read into buffers in node memory as described under BUFSW measurement. If there are no buffers available when a buffer switch is attempted, this count is pegged. Any messages not read are then transmitted via direct memory access into the "throw away" portion of the node processor memory (effectively discarding them). This count should always be the same as the RRBOVFLW3 count.
INIT0 (Office)	Number of level 0 IMS initializations that started. Level 0 is the audit level. When invoked either automatically or manually, the selected audit starts. Should a critical audit fail, the initialization may escalate to level 1B. At level 0, the message switch is running. The IMS initialization levels are basically the same as the corresponding application and operating system levels.
INIT0T (Office)	Duration of level 0 IMS initialization. Since the initialization sequence for level 0, 1A, and 1B do not recreate any IMS processes, these durations are exclusive of the boot prologue and the boot level initializations.
INIT1A (Office)	Number of level 1A IMS initializations that started. This is the recovery level and may be triggered by internal problems. Tables are rebuilt from information in the central processor and ring nodes. A level one system initialization triggers either an IMS level 1A or 1B. During level 1A, IMS is capable of switching messages, but messages may be lost due to audits and reinitialization of communications between the central processor and ring. It may escalate to level 1B.
INIT1AT (Office)	Duration of level 1A IMS initialization (see INIT0T description).
INIT1B (Office)	Number of level 1B IMS initializations that started. During level 1B, IMS is not capable of switching messages (messages are lost).
INIT1BT (Office)	Duration of level 1B IMS initialization. Refer to INIT0T description.
INIT2 (Office)	Number of level 2 IMS initializations started. This level immediately escalates to level 3.
INIT2T (Office)	Duration of level 2 IMS initialization. Refer to the INIT3T description.
INIT3 (Office)	Number of level 3 IMS initializations that started. This is the lowest boot level. If the boot is unsuccessful, CNI and IMS abort. If possible, the previously existing ring configuration is maintained (if necessary, a quick reconfiguration is attempted). Selected nodes may be downloaded.
INIT3T (Office)	Duration of level 3 IMS initialization. The boot level initialization durations do not include the time spent aborting IMS, the time spent recreating the driver, nor the time spent in the boot prologue.
INIT4 (Office)	Number of level 4 IMS initializations that started. This is the highest boot level. If the boot is unsuccessful due to a software problem, CNI and IMS abort. If the boot is unsuccessful due

	to a hardware problem, IMS is still capable of performing diagnostics. If the boot is successful, all ring nodes are downloaded. It allows the system to operate even if no usable ring configuration is established. Automatic recovery can be inhibited.
INIT4T (Office)	Duration of level 4 IMS initializations. Refer to INIT3T description.
INITBT (Office)	Number of IMS boot prologues that start. This counts how many times IMS is booted (recreated), whereas the initialization levels 2, 3, and 4 counts indicate how many times the boot loads to those particular sequences. If an initialization fails, it may be retried automatically. Since level 2 invokes level 3, the sum of INIT2 and INIT3 and INIT4 could exceed this count.
INITBTT (Office)	Duration of IMS boot prologue. This measurement begins when the IMS driver is created. It is exclusive of the boot level initialization durations.
IPFMTER0 (NP)	Ring input format error on ring 0. This error is detected at the input to the ring access circuit. It occurs when a message passing through the ring access circuit buffer has format problems. This condition is checked even if the message is not read by the node. Furthermore, the format error is also pegged by the RDFMTER0 count when the message is read.
IPMTER1 (NP)	Ring input format error on ring 1 (see IPFMTER0).
IPSM0 (NP)	Ring 0 input source match. When a message on the ring is not dequeued by the node it is destined for, the message continues to traverse the ring to the sending node. The sender then detects the message, removes and discards it, and notifies the central processor. This count is pegged for the destination node.
IPSM1 (NP)	Ring 1 input source match. Refer to IPSM0 description.
IUNOVL0 (IUN)	Number of times the IMS user node entered overload level 0 (the normal state). The IUNOVL0_ measurements indicate the number of times the node is in a state in which all available central processor unit time is consumed (refer to IDLE description). Entering this state indicates the processor is idle and pegs when the node processor returns to level 0 from level 1 or 2.
IUNOVL1 (IUN)	Number of times the IMS user node entered overload level 1. The node processor has not been idle for some time and messages from the user apparatus is processed on a "clocked" schedule to reduce NP load.
IUNOVL2 (IUN)	Number of times the IMS user node entered overload level 2. The node processor has not been idle for a longer period of time and messages from the ring to the user apparatus are processed on a "clocked" schedule to further reduce NP load.
MINTRA (RPC)	Number of intranode messages delivered. Within a ring peripheral controller node, there are different processes communicating with the 3B20D computer and the ring. When a message is sent between the ring and the central processor, these processes must transfer the message from one to another. This measurement is a count of messages transferred without the node. It is not strictly a count of messages transferred between the central processor and the ring, but is at least the sum of the RTOCUMSG and the CUTORMSG measurements.
MRINTCH (NP)	Message returned to the ring due to destination channel being closed. When a message is sent to a closed channel in a node, the message must be returned (refer to RINTCH description). The count is a cumulative total for all channels in the node, while RINTCH is counted per channel in the central processor.
MRNIAU (Office)	Automatic multiple ring node isolation. When a node is isolated, the ring is reconfigured to group all isolated nodes into one isolated segment. The nodes involved may have been isolated automatically, manually, or as an innocent victim of the ring reconfiguration. If the segment has more than one node and the most recently isolated node is isolated by automatic action, the entire segment is considered to be isolated automatically. This count is pegged when the ring is successfully reconfigured automatically and the node is isolated.
MRNIAUT (Office)	Duration of automatic multiple ring node isolation. This is the cumulative time in which an automatically generated ring configuration exists with more than one node isolated.
MRNRING (NP)	Message returned from ring. When the node receives a message that is not accepted by the destination (the return message control code is detected), the message is discarded and this count is pegged. See MRRING, RINTCH, and MRINTCH descriptions for reasons messages are returned.
MRRGQ0 (NP)	Message received from ring 0 queued. In the node processor, messages received from the ring are placed in one of the ring receive buffers in memory. A separate list of pointers (queue) to the messages in the buffers is maintained for each channel (except in-place channels). This count is the cumulative total of all messages from ring 0 queued for any of

	these channels. At a ring peripheral controller, this count is the number of blocks given to the active ring channel. A block may contain several messages. For in-place channels, messages are processed in the buffers. After processing, these messages may be queued to be read by some other channel.
MRGQ1 (NP)	Message received from ring 1 queued. Refer to MRGQ0 description.
MRRING (Office)	Message returned to ring with "returned message" control code (destination did not accept message). This count is the number of times messages are returned to the ring because of destination channel not open, the destination's read queue is full, or there is no buffer space for the message. If the message is not already a returned message, this count is pegged. The "returned message" control code is then added to the message; source and destination addresses are swapped; and the message sent to the ring. If the message is already a returned message, it is discarded and this count is unaffected.
MXRG0 (NP)	Message transmitted to ring 0. When a message is to be transmitted to the ring, a pointer to the buffer in the node processor memory containing the message is placed on queue. The queue represents a block of messages to be transmitted by the direct memory access to the ring. This count is incremented by the number of messages in the block to be sent to ring 0.
MRRG1 (NP)	Message transmitted to ring 1. Refer to MXRG0 description.
NPPTER (NP)	Node processor parity error. This count is pegged when the node reports an internal memory parity error. The error results in the node processor putting itself in a quarantine state and is not reported to the central processor. <i>This count is presently ineffective and should always be zero.</i>
OOSAU (NP)	Automatic out of service. This count is the number of times the node has entered either the out-of-service state or standby state due to automatic action. This could be because of failing diagnostics or some automatically detected fault. The node maintenance state may later change to manual; but, until the major state changes, it is considered to be automatic out of service. This count does not peg if the node is an innocent victim of a ring reconfiguration (see the OOSCFG description).
OOSAUT (NP)	Duration of automatic out of service. This is the cumulative total of the times the node is in this state.
OOSCFG (NP)	Out of service due to ring reconfiguration. This count is the number of times the node has entered either the out-of-service state or standby state due to automatic action and because it is an innocent victim of a ring reconfiguration. When the node first enters this maintenance state, it is isolated and may later change to manual; but, until the major state changes, it is considered to be automatic out of service. This count also includes those situations where the node is removed from service due to the entire ring down or ring reconfiguration in progress.
OSCFGT (NP)	Duration out of service due to ring reconfiguration. This is the cumulative total of times the node is in this state.
OOSMN (NP)	Manual out of service. This count is the number of times the node has entered either the out-of-service state or standby state due to manual action. The node maintenance state may later change to automatic; but, until the major state changes, it is considered to be manual out of service.
OOSMT (NP)	Duration of manual out of service. This is the cumulative total of times the node is in this state.
PANICS (NP)	Number of recoverable errors. There are conditions that force the node processor to restart. If the condition does not halt processing, it is called a soft error and this count pegs. If the processor must be rebooted, it is called a hard error and it does not effect this count. (It does not peg since error logging is not possible.)
PIOFLT (RPC/DLN)	Fault recovered after a program input/output request is issued to a ring peripheral controller. The program input/output is used by the central processor mostly for sending commands to the ring peripheral controller and for receiving status information from the ring peripheral controller. There are two types of requests used: • Hardware (to cause some hardware action) • Software (to send a command to some process).

	Both of these requests wait for the program input/output request to complete. If the hardware detects a fault during the input/output, this error is reported to the central processor and the count is pegged.
PTERTE (NP)	Number of times soft parity error exceeded a threshold. A cumulative count of both SEPTER0 and SEPTER1 is kept by the central processor. When that count exceeds a threshold, this count is pegged and a ring reconfiguration is triggered to isolate the offending node.
RACER0 (NP)	Ring access controller problem on ring 0. The ring access controller has a set of condition bits in its status ports that indicate trouble in the ring access controller. When the node processor observes problems in the ring access controller for ring 0 (indicated by condition bits), it attempts to clear the problem for a maximum of 10 retries. If unsuccessful, this error report is issued to the central processor and the count is pegged.
RACER1 (NP)	Ring access controller problem in ring 1. Refer to RACER0 description.
RBOF (CHN)	Single message read list buffer overflow. Each central processor channel using single message read mode is allowed a single message read list. This list contains pointers to the message defined for this channel. The message is actually contained in a buffer from a pool of buffers shared among all single message read list users. The message switch tries to deliver a message to the channel by placing a pointer in the read list. If all pointer slots in the read list contain pointers to messages waiting to be read by the channel owner, the count pegs. This is an indication that messages are being queued faster than the owner of the channel can read them.
RBOFBLK (CHN)	Block message read list buffer overflow. This count is the block mode equivalent of the RBOF count. A central processor channel using block read mode is allocated a block read list (or buffer). This structure is actually just buffer space to hold messages destined for this channel. The buffer is allocated from a common pool. The actual message is copied into the channel's private buffer space. If there is not room in the buffer to hold a new message for this channel (the read list is full), the message switch pegs this count. Block read buffers are circular; if there is room, messages are put after the last message delivered and before the oldest message still being used.
RCOPTER0 (NP)	Ring access controller output parity error on ring 0. This parity error is generated in the node processor when a message from the ring access controller for ring 0 is read into node processor memory. Since parity is good when the data is transferred into the ring access controller, the problem is internal to the ring access controller.
RCOPTER1 (NP)	Ring access controller output parity error on ring 1. Refer to RCOPTER0 description.
RDFMTER0 (NP)	Ring read format error on ring 0. Read format errors are detected in the ring access controller buffer during the reading of the message into the node processor memory and are usually due to partial or truncated messages received by the node. The size specified in the header is greater than the actual message size received. Unless the node is a ring peripheral controller, read format errors are not generated when a broadcast message is involved.
RDFMTER1 (NP)	Ring read format error on ring 1. Refer to RDFMTER0 description.
RDINHER0 (NP)	Read inhibit error on ring 0. Data in the ring access controller is read into the node processor by direct memory access. The node contains a timer that allows a specific time for the read operation. If after the timer expires and no data has been transferred, the node reports this error to the central processor and the count is pegged.
RDINHER1 (NP)	Read inhibit error on ring 1. Refer to RDINHER0 description.
RDWN (Office)	Entire ring down. This count is pegged whenever the ring maintenance state is changed to indicate the entire ring is down (unable to process messages). All nodes peg either the OOSAU, OOSCFG, or OOSMN count when this occurs depending on their maintenance state.
RDWNT (Office)	Duration of that entire ring is down. This is the cumulative total of the time the ring is in the down state.
RGCNFG (Office)	Ring containing an isolated segment. This count pegs when an isolated segment is unsuccessfully established either by manual or automatic action. This count is the sum of SRNIAU, MRNIAU, and RNIMN counts.
RGNCNFGT (Office)	Duration of ring contains an isolated segment. This is the cumulative time during which the ring had at least one node isolated or the sum of SNIAUT, MRNAUT, and RNIMNT counts.
RINTCH (CHN)	Message returned to the ring due to closed destination channel in the central processor. If the message is already a returned message, it is discarded and this count is not pegged.

	Otherwise, the "returned message" control code is added to the message, source, and destination addresses are swapped, the message is sent to the ring, and the count is pegged.
RIPTER0 (NP)	Ring interface parity error or orphan byte condition on ring 0. This count is pegged if the parity error exists after retry (refer to SEPTER0 count). The node does not accept the data which usually results in a corresponding blockage report from the upstream node.
RIPTER1 (NP)	Ring interface parity error or orphan byte condition on ring 1. See the RIPTER0 description.
RNIMN (Office)	Zero or more ring nodes isolated manually. This count is similar to the MRNAIAU count except it is caused by manual action. If the most recent isolation is by manual action, the entire isolated segment is considered to be isolated manually. An isolated segment with zero nodes is possible when growing nodes. Unequipped nodes are isolated by placing the BISO and EISO nodes around the unequipped nodes. After the nodes are grown and diagnosed, automatic ring recovery restores them to service and the isolated segment disappears. This count is pegged when the ring is successfully reconfigured manually and the segment is isolated.
RNIMNT (Office)	Duration of zero or more ring nodes isolated manually (see the RNIMN description for an explanation of zero nodes isolated). This is the cumulative time that a manually generated ring configuration exists with an isolated segment.
RPCBOF (RPC)	Ring peripheral controller buffer overflow. The message switch sends and receives messages to the ring by direct memory access channels to the ring peripheral controller. During each message switch cycle, the ring peripheral controller sends messages in buffer to the central processor and the central processor sends messages to the ring peripheral controller buffer. This count pegs when the message switch tries to add a message to the buffer when it is full.
RRBOVFLW0 (NP)	Number of times the ring node has reached the overflow state 0 (the normal, no discard state). Messages in the ring receive buffers are being processed at least as fast as they are being received. If the node is a ring peripheral controller, all IMS user nodes associated with it are notified of the nodes overflow state.
RRBOVFLW1 (NP)	Number of times the ring node has transitioned to the overflow state 1. Messages are being received faster than they can be processed and buffer occupancy has exceeded the threshold for overflow. In state 1, a warning of imminent overflow is sent.
RRBOVFLW1T (NP)	Duration of ring receive buffer overflow state 1.
RBOVFLW2 (NP)	Number of times a ring node reached the overflow state 2. In state 2, non-IMS messages are discarded in the ring nodes only (all ring nodes are notified of the home ring peripheral controller overflow state). The IMS does not allow non-IMS messages to be written to a home peripheral controller that is in overflow state 2 or 3. When any ring node is in overflow state 2, any non-IMS messages read from the ring are discarded.
RRBOVFLW2T (NP)	Duration of ring receiver buffer overflow state 2.
RRBOVFLW3 (NP)	Number of times the ring node has reached the overflow state 3. In state 3, the node is in the "throw away" mode. In this state, all messages for link nodes and ring peripheral controller direct memory access are read into a throw away area of memory (effectively discarded).
RRBOVFLW3T (NP)	Duration of ring receive buffer overflow state 3.
RSTRMT (NP)	Successful restart without reload.
RTMSGSRC (LN)	Message received with a source address match. If a message sent by this node has traversed the entire ring without being taken, the ring interface hardware detects a match of the source address. When the match occurs, the message is removed from the ring. If the message is not a broadcast message, this count is pegged and a report is sent to the central processor (see the IPSM description).
RTOCUMSG (RPC)	Ring peripheral controller to 3B20D computer IMS messages. This measurement is a cumulative count of messages received by the central processor from a specific ring peripheral controller. It is similar to the CUTORMSG count.
PTOCUWDS (RPC)	Ring peripheral controller to 3B20D computer IMS messages words. Each message read from or written to the ring is composed of a number of 3B20D computer words (varies with message type and data contained). It is similar to the CUTORWDS count.
SFPTER0 (NP)	Soft parity error on ring 0. This parity error is generated in a ring access controller while receiving data. After detecting this error, the node requests the ring access controller to retry the parity error check. If the parity condition is gone, this count is pegged and the error is considered transient. If the parity condition still exists, the node considers it to be a hard parity (refer to RIPTER0 description).

SFPTER1 (NP)	Soft parity error on ring 1. Refer to SEPTER0 description.
SPNIAU (Office)	Automatic single ring node isolation. This count is similar to the MRNIAU count. If an isolated segment has only one node that is isolated by automatic action, the segment is considered to be isolated automatically. This count is pegged when the ring is successfully reconfigured and the node is isolated.
SRNIAUT (Office)	Duration of automatic single ring node isolation. This is the cumulative time in which an automatically generated ring configuration exists with a single node isolated.
WBOFN (CHN)	New write list buffer overflow. Each IMS central processor channel that originates messages is allocated a buffer (the new write list) for building messages. When a message is to be built, a request is made for space in this buffer. If the request exceeds the available space in the buffer, the write list overflows, and this count is pegged. This is an indication that the destination ring peripheral controller has not finished a previous direct memory access transmission. Normally, the message switch empties the write buffer each cycle.
WBOFNL (CHN)	Long new write list buffer overflow. This is the long buffer equivalent of the WBOFN count. The buffers used for long write lists are separate from those used for the short write list. This count is pegged if the request for space in a long buffer exceeds the available space. This is an indication that the destination ring peripheral controller has not finished a previous direct memory access transmission. Normally, the message switch empties the write buffer each cycle.
WBOFO (CHN)	Old write list buffer overflow. The buffers used to write old messages are the same buffers used to read messages. The messages are read, processed in place, and then written. Each channel is allocated a list of pointers to the buffers containing the messages. When too many messages are waiting, this overflow count pegs. This is an indication that the destination ring peripheral controller has not finished a previous direct memory access transmission. Normally, the message switch empties the write buffer each cycle.
WRRGQ0 (NP)	3B20D computer words received from ring 0 queued. This count is the cumulative total of the number of words in all messages from ring 0 queued for any channel. Refer to MRRGQ0 description.
WRRGQ1 (NP)	3B20D computer words received from ring 1 queued. This count is the cumulative total of the number of words in all messages from ring 1 queued for any channel. Refer to MRRGQ1 description.
WSMER0 (NP)	Write source match error on ring 0. The source address in a message being written to the ring does not match the node's address as specified in the ring interface hardware. Since the WSMER condition is counted against the WTFMTER count, this count should always be 0.
WSMER1 (NP)	Write source match error on ring 1. Refer to WSMER0 description.
WTFMTER0 (NP)	Ring write format error on ring 0. When the token is detected in the ring access controller, the node begins transmitting any messages that have queued. This error is detected while attempting to write to the ring. If the source address in a message being written does not match the node's address as specified in the ring interface hardware or the message is too short to contain a valid header, it is reported to the control processor, this count is pegged, and the write is inhibited. The buffer that is being sent to the ring is discarded.
WTFMTER1 (NP)	Ring write format error on ring 1. Refer to the WTFMTER0 description.
WXRG0 (NP)	3B20D computer words transmitted to ring 0. This count is incremented by the number of words transmitted via direct memory access to ring 0 as described under MXRG0 count.
WXRG1 (NP)	3B20D computer words transmitted to ring 1. This count is incremented by the number of words transmitted via direct memory access to ring 1 as described in MXRG1 count.

Table 3.13.1-2 SS7 CNI Measurement Descriptions

NAME (TYPE)	DESCRIPTION
ALSR (SS7)	Number of alternate link set transitions to a lower priority link.
ALSRT (SS7)	Duration of alternate link set transitions to a lower priority link.
ALSRO (SS7)	Total number of alternate link set routing transitions to a lower priority link.
ALSROT (SS7)	Total duration of alternate link set transitions to a lower priority link.
BYMSUR (SS7)	Message signal unit bytes received. This count, along with the BYMSUX, MGMSUR, and MGMSUX counts, provide a good measure of traffic flow on the link. A message signal unit contains CCS message data (refer to MGMSUR count for a description of the type of signal units). When a message signal unit is received, this count is incremented in the link interface by the length of the signal unit in bytes (not including flags between

	signal units).
BYMSUX (SS7)	Message signal unit bytes transmitted. Refer to BYMSUR description.
BYR (SS7)	Total bytes received excluding flags. Data is transmitted over SS7 links using signal units. All signal units have at least one flag byte at the end to delimit between signal units. All signal units contain a header and check bits. When any level 2 or 3 type signal unit is received, these flag bytes are removed and this count is incremented in the link interface by the length of the signal unit in bytes. The BYMSUR measurement is included in this measurement. Furthermore, this count includes bytes from all types of signal units. Therefore, it is usually a large value. This count does not include bytes received in error.
BYRX (SS7)	Retransmitted bytes including flags. Signal units are composed of varying numbers of bytes depending on the type of signal unit and the data contained. Only message signal units are retransmitted. Should the node determine a signal unit must be retransmitted, this count is incremented in the link interface by the number of bytes sent. This would be the number of bytes in the erroneous signal unit and any subsequent signal units not positively acknowledged.
BYRXTE (SS7)	Threshold exceeded for BYRX. When the BYRX count has exceeded a certain value, this count pegs. It indicates too many signal units are being retransmitted. This could be due to synchronization problem (refer to the L7FLALIGN count) or due to the far-end receiving signal units in error.
BYSR (SS7)	Non-ECIS bytes received excluding flags. Messages are transmitted over SS7 links in message signal units. These signal units are composed of varying numbers of bytes. Each signal unit includes a header, check bits, and at least one flag (removed by the link interface). When the node receives a message signal unit containing message data other than ECIS6, this count is incremented by the length of the signal unit in bytes. This measurement is usually a large value.
BYSX (SS7)	Non-ECIS bytes transmitted. See RYSR description.
BYX (SS7)	Total bytes transmitted excluding flags. This measurement includes any bytes due to retransmitted messages. Note that since the BYR count does not include bytes of signal units received in error, this count may differ from the BYR count at the far-end. Refer to the BYR description for more details.
CLF (Link Set)	Link set failure. When the last available link in the set fails, this count pegs and the appropriate trunk failure messages are sent. This count indicates how many times the link set failed. Refer to CLFA, CLFB, and CLFC descriptions for more details on specific link set failure. Note that the failure of a link set may result in a signaling point isolation.
CLFA (Office)	A-link set failure. This is a cumulative total of the CLF count for all A-link sets in the office.
CLFAT (Office)	Duration of A-link set failure.
CLFSP (Office)	Link set failure. This is a cumulative count of all link set failures in the office. See CLF duration.
CLFSPT (Office)	Duration of link set failure. This count is a cumulative duration of all link set failures in the office. See CLFT description.
COS7CRFSRCM (SS7)	Number of times a CREF message is sent due to a source match.
COS7DCHNOOS (SS7)	Number of times an incoming CO-SCCP message is discarded due to destination D-channel being out of service.
COS7DSDSRCM (SS7)	Number of times a CO-SCCP message is discarded due to source match.
COS7ERRSRCM (SS7)	Number of times an ERROR message is sent due to a source match.
COS7LCNINV (SS7)	Number of times an incoming CO-SCCP message is discarded due to an invalid or unequipped LACID.
COS7RLCSRCM (SS7)	Number of times an RLC message is sent due to source match.
CRCER (SS7)	Cyclic redundancy check errors. The link interface checks for data errors in received signal units using the check bits that are part of a received signal unit. If the CRC check fails, the signal unit is discarded, the count is pegged, and a negative acknowledgement is sent. When the rate of these errors exceeds a predetermined value, the node is notified and the link is marked as failed.
CRCERTE (SS7)	Threshold exceeded for CRCER. When the CRCER count exceeds a certain value, this count pegs. It is an indication that the data link carrier failed.
DDCLFLABN (SS7)	Cumulative duration of signaling link declared failures due to abnormal condition. This count pegs in the central processor.

DDFLHWP (SS7)	Cumulative duration of signaling link declared failure due to general hardware problems. This count pegs in the central processor.
DDCFLSWP (SS7)	Cumulative duration of signaling link declared failures due to general software problems. This count pegs in the central processor.
DDCFLXDA (SS7)	Cumulative duration of signaling link declared failures due to excessive delay of acknowledgement. This count pegs in the central processor.
DDCFLDC (SS7)	Cumulative duration of signaling link declared failures due to excessive congestion durations. This count pegs in the central processor.
DDCFLXER (SS7)	Cumulative duration of signaling link declared failures due to excessive error rate. This count pegs in the central processor.
DRLNKUNV	Total duration of link unavailability for user traffic.
DRP7MSG1 (SS7)	Number of priority level 1 messages dropped due to ring peripheral controller congestion. The node examines the service information field in the message to determine its priority before sending it on the ring. Except for ECIS6 messages, this count is the cumulative total of all messages discarded due to level 1 ring peripheral controller congestion.
DRP7MSG2 (SS7)	Number of priority level 2 messages dropped due to ring peripheral controller congestion. The count is similar to the DRP7MSG1 count and is the cumulative total of all messages discarded due to level 2 ring peripheral controller congestion.
DRP7MSG3 (SS7)	Number of priority level 3 messages dropped due to ring peripheral controller congestion. This count is similar to DRP7MSG1 count and is the cumulative total of all messages discarded due to level 3 ring peripheral controller congestion.
DRPEMSG1 (SS7)	Number of priority level 1 ECIS6 messages dropped due to ring peripheral controller congestion. This count pegs for any ECIS6 message discarded due to level 1 ring peripheral controller congestion. The DRPEMSG_counts are not included in the DRP7MSG counts.
DRPEMSG2 (SS7)	Number of priority level 2 ECIS6 messages dropped due to ring peripheral controller congestion.
DRPEMSG3 (SS7)	Number of priority level 3 ECIS6 messages dropped due to ring peripheral controller congestion.
ERSEC (SS7)	Number of 1-second intervals with at least one error. Each second, the link interface determines if any signal units have been received in error. The count pegs if there are any errors during a second; it is not a count of the number of errors.
ERSECTE (SS7)	Threshold exceeded for ERSEC. When the ERSEC count has exceeded a certain value, this count pegs. The error is an indication of facility performance degradation.
FORRX (SS7)	The link experienced a forced retransmit cycle. When the far-end indicated received errors, the affected messages are retransmitted at the time the count pegs in the link interface. A large number of forced retransmit cycles can cause transmit buffer congestion and discarding of messages. This count indicates high queuing delays which could cause a reduction in throughput.
FORRXBY (SS7)	Bytes retransmitted during forced retransmit mode. This count is pegged in the link interface and is the cumulative total of bytes transmitted during forced retransmit cycles.
GTTPERFD (Office)	Total number of SS7 global title translations performed by the signaling connection control part (SCCP) in the central processor.
GTTUNBC (Office)	Global title translation could not be performed due to congestion.
GTTUNNT (Office)	Global title translation could not be performed due to congestion.
GTTUNONS	Global title translations unable to perform diagnostic 0. No translations for address of such nature.
HTXNEGAK (SS7)	Link unavailable. This is the sum of L7AFLT and L7MFLT. A relative measure indicating the percentage of time the link is out of service (0 to 100 percent).
L6MGRV_ (SS7)	ECIS6 messages received on virtual link. Since ECIS messages are the only banded messages received on an SS7 link, this is the total count of all banded messages received for the indicated virtual link. These messages are not included in the total SS7 messages received (L7MGSR count). This count includes initial address (MGIAMRV_) and answer (MGANSRV_) messages.
L6MGXV_ (SS7)	ECIS6 messages transmitted on virtual link. Since ECIS messages are the only banded messages transmitted on the SS7 link, this is the total of all banded messages transmitted for the indicated virtual link. It includes the MGIAMX_ and MGANSX_ counts.
L6SUPRV (SS7)	Telephone message signal units received on virtual link. This is the total count of all

	signal units involved in banded messages received for the indicated virtual link.
L6SUPXV_ (SS7)	Telephone message signal units transmitted on virtual link. Since ECIS messages are the only banded messages transmitted on an SS7 link, this is the total count of all signal units involved in banded messages transmitted for the indicated virtual link. This count does not include SYNC, ACU, or PRO signal units.
L7ACO (SS7)	Automatic changeover. This is the sum of near-end (L7ACONE) and far-end (L7ACOFE) changeovers.
L7ACOTE (SS7)	Automatic changeover threshold exceeded. When the L7ACO count has exceeded a certain value, this count pegs. The link is experiencing excessive errors causing repeated changeovers to another link.
L7ACOFE (SS7)	Automatic changeover initiated by the far-end. The changeover involves transferring signaling messages from the unavailable link to any link in the combined link set or C-links. A C-link changeover causes messages to be load balanced between any other available C-links. Both the changeover order and acknowledgement are sent on another link in the specified link's set. When the order is received from the far-end, this count pegs and either a changeover or emergency changeover is initiated. The latter is used when the node is out of service, or the far-end indicates out of sequence messages. Following is the changeover sequence. (1) The link is removed from service and no new messages are given to the node. (2) Messages remaining in the transmit/retransmit buffer are retrieved and sent in sequence on other links. An emergency cutover does not attempt to retrieve messages from the retransmit buffer. If the link node is out of service, the link failed due to near-end PRO, or the far-end is blocked by the failure, no messages are retrieved. (3) Message handling resumes with new messages sent to the other links and only synchronization signal units sent on this link. If the cutover is automatic, the link changes back when synchronism is restored. If the link cannot sync and change back within 3 minutes (10 minutes if long key exchange is involved), it is declared failed and the L7FLD count pegs.
L7ACONE (SS7)	Automatic changeovers initiated at the near-end. This occurs usually due to excessive errors on the link. If all links in the combined link set are out of service or the C-links are unable to handle the additional load, an EMR occurs and changeover is denied. If allowed, this count pegs and either a changeover or emergency changeover is initiated. The sequence is described under L7ACOFE measurement. The sequence indicated is followed, except a changeover order is sent to the far-end rather than being received. All acknowledgements must be received before starting the changeover.
L7AFLT (SS7)	Duration of automatic link out of service including duration of declared failure. Refer to L6AFLT description.
L7BADRTG (SS7)	Message signal units discarded due to bad or no routing data. If the translation for a receive DCIS6 message fails due to no translation data, it is discarded in the incoming node, this count is pegged, and the UDS message is returned to the originator. If a received non-DCIS6 message has a destination point code associated with an outgoing CCIS6 pool, it is discarded in the incoming node and this count is pegged. Refer to the MRSNTO7 count for a total number of DCIS6 messages discarded in the central processor due to translation failure.
L7BOFR (SS7)	The receive buffer in an SS7 link node overflows. Refer to the L6BOFR description.
L7BOFRT (SS7)	Duration of the receive buffer overflow. This timer pegs in the link interface. Refer to L6BOFRT description.
L7BOLR (SS7)	The receive buffer in an SS7 link node overloaded. Refer to the L6BOLR count for a description of buffer overload. No messages are discarded in the overload state. When overload occurs, the link interface stops transmitting positive acknowledgements to the

	far-end until the congestion is relieved. The far-end responds by limiting traffic to the near-end.
L7BOLRT (SS7)	Duration of the receive buffer overload. This timer pegs in the link interface.
L7BYTO3B (SS7)	SS7 message bytes sent to 3B20D computer. This count is incremented by the size of the message when it is sent to the central processor.
L7DIF (SS7)	CNI SS7 data integrity flag. Refer to L6DIF.
L7EMER (SS7)	Emergency restart due to local failure. This count pegs only if there are virtual links assigned to the indicated SS7 link. Refer to the EMR description.
L7EMRPO (SS7)	Emergency restart due to far-end processor outage. This count pegs only if there are virtual links assigned to the indicated SS7 link. Refer to EMRPO description.
L7EMRPOT (SS7)	Duration of emergency restart due to far-end processor outage.
L7EMPT (SS7)	Duration of emergency restart due to local failure.
L7FLALIGN (SS7)	Alignment failure. This count indicates the number of signal units received in error during the initial alignment procedure. This procedure is the first part of the level 2 protocol and is done once when a link is restored. When a link is out of alignment, the link is sending only status signal units indicating that fact. Once alignment is achieved, the link begins a prove-in period. During the prove-in, the error rate monitor counts signal units received in error. Once prove-in is complete, the link is ready and traffic may start. This link interface now reports the error rate, and the value is accumulated into this count.
L7FLD (SS7)	Declared link failure. A declared failure could be due to a 1-minute continuous buffer overload, a sanity check failure, a 30-second far-end processor congestion, or a changeover lasting more than 3 minutes (10 minutes if a long key exchange is involved). The changeover could be due to far-end request or because errors exceeded the threshold for changeover. This count pegs and the appropriate TFX or TCX messages are broadcast. The link is diagnosed if failure is due to a far-end PRO (diagnostics wait until the outage ends). This failure could also cause the combined link set to fail (refer to CLF measurement). Some of the actions leading to declared failure are described in the L7BOLR, L7ACOF, L7CR, and CRCL descriptions.
L7FLDT (SS7)	Duration of declared link failure.
L7LCDIS1X (SS7)	Level 1 transmit buffer congestion discard. This count is the number of times the transmit buffer occupancy reached the indicated threshold for message discard. Selected messages are being discarded according to the strategy described under the MSURMV measurement. Since the corresponding onset level has been reached, far-end signaling points are also discarding messages according to the strategy because of the receipt of transfer controlled messages. This count does not peg again at least until occupancy drops below the corresponding threshold.
L7LCDIS1XT (SS7)	Duration of level 1 congestion discard.
L7LCDIS2X (SS7)	Level 2 transmit buffer congestion discard. This is the next higher discard level from discard level 1.
L7LCDIS2XT (SS7)	Duration of level 2 discard.
L7LCDIS3X (SS7)	Level 3 transmit buffer congestion discard. This is the next higher level from discard 2 and is the highest discard level possible.
L7LCDIS3XT (SS7)	Duration of level 3 congestion discard.
L7LCON1X (SS7)	Level 1 transmit buffer congestion onset. This count is the number of times the transmit buffer occupancy reached the indicated threshold for congestion (the congestion level is higher than the corresponding acceptable level but lower than the corresponding discard level). At each onset level, the node reports the congestion state to the central processor. Network management messages are then broadcast to adjacent signaling points to limit messages to the affected node. To avoid further congestion of the transmit buffer, the far-end initiates the discard strategy used by nodes at the discard level.
L7CON1XT (SS7)	Duration of level 1 congestion onset. This time period includes level 2 and 3 also. If the node remains in the same congestion level (1, 2, or 3) for 60 seconds, it is taken out of service and diagnosed. However, since the duration timers for each level are cumulative, they may exceed the 60-second limit.
L7LCON2X (SS7)	Level 2 transmit buffer congestion onset. Messages are being discarded according to the level 1 strategy. The node reports the level 2 congestion state to the central processor. Actions are taken as described under the L7LCON1X measurement.
L7LCON2XT (SS7)	Duration of level 2 congestion onset. This time period includes level 3 also.

L7LCON3X (SS7)	Level 3 transmit buffer congestion onset. Messages are being discarded according to the level 2 strategy. The node reports the level 3 congestion state to the central processor. Actions are taken as described under the L7LCON1X measurement.
L7CON3XT (SS7)	Duration of level congestion onset.
L7MCOFE (SS7)	Far-end manual changeover request has been received, usually due to a need for link changes or maintenance. The far-end has requested and permission has been granted to initiate a changeover. Either a changeover or emergency changeover is initiated. The sequence is described under L7ACOFE description.
L7MCONE (SS7)	Near-end manual changeover due to local maintenance action. The changeover could be denied if removing the link from service would cause the far-end to become inaccessible. This end requests permission from the far-end to initiate a changeover (the far-end pegs the L7MCOFE count). If the far-end grants permission, either a changeover or emergency changeover is initiated. The sequence is described under the L7ACOFE description. The sequence indicated is followed, except, a changeover request is sent to the far-end rather than being received. All acknowledgements must be received before starting the changeover.
L7MFLT (SS7)	Duration of manual link out of service.
L7MGSR (SS7)	Non-ECIS6 messages received. This count includes only SCCP and network management messages. The count pegs in the node when the message is received from the link interface.
L7MG SX (SS7)	Non-ECIS6 messages transmitted. Refer to L7MGSR description.
L7MRPBC (SS7)	ECIS6 message rejected due to congestion. Bonded messages are transmitted in SS7 links using ECIS6 protocol. This count is a cumulative total for all virtual links assigned to the indicated link.
L7MRPNT (SS7)	ECIS6 message rejected due to translation data. Bonded messages are transmitted on SS7 links using ECIS6 protocol. This count is a cumulative total of all virtual links assigned to the indicated link.
L7POR (SS7)	Far-end processor outage occurred. This is not a count of the number of processor outage signal units received. It is a count of the number of processor outage events recognized by the specified link. When the far-end office sends the message, it indicates that office is undergoing initialization or is overloaded. The far-end link interface is in the processor outage send mode. The problem is treated as a link failure. This count pegs once when the first processor signal unit is received and not again at least until the processor outage signal units stop.
L7PORT (SS7)	Duration of processor outage.
L7POX (SS7)	Link interface in processor outage send mode. This link status signal units indicate the processor outage condition.
L7POXT (SS7)	Duration of processor outage in effect. This timer pegs in the link interface.
L7RBFOC (SS7)	Average receive buffer length in bytes. This is the average occupancy of the buffer and is obtained by periodically checking buffer length, cumulating the number of bytes, and dividing by the number of times the length is checked. Since this is a measure of how long messages are staying in the buffer, it is a relative measure of the load on the link. This count pegs in the link interface.
L7RTGAUD (SS7)	Routing audit failure. This is an automatic audit that checks consistency of the pool to point code table every 10 seconds. The active 3B20D computer data is checked first. If errors are found, an output message is generated and the errors corrected. Next, the data is checked in all SS7 nodes. When the pool to point code audit finds errors in the node, they are corrected and this count pegs.
L7XBFOC (SS7)	Number of transmit buffer visits by the link interface. This is the number of times the link interface checked buffer occupancy in order to calculate the L7XBFOC and L7RBFOC counts. This count pegs in the link interface.
L7XBFOC (SS7)	Average transmit buffer length in bytes. Refer to L6XBFOC description.
LINKDLAY	Average link output delay for sampled MSUs.
MGANSRV_ (SS7)	Answer messages received on virtual link. This measurement is the total count of all answer messages received for the indicated virtual link. Refer to the MGANSR description.
MGANSXV_ (SS7)	Answer messages transmitted on virtual link. This measurement is the total count of all answer messages transmitted for the indicated virtual link. Refer to the MGIAMR description.

MGIAMRV_ (SS7)	Initial address messages received on virtual link. This is the total count of all initial address messages received for the indicated virtual link. Refer to MGIAMR description.
MGIAMXV_ (SS7)	Initial address messages transmitted on virtual link. This is the total count of all initial address messages transmitted for the indicated virtual link. Refer to MGIAMX description.
MGMSUR (SS7)	Message signal units received. Data is transmitted over SS7 links using three types of signal units: Level 3 - Message signal units containing CCS message information (these are passed to and from the node). Level 2 - Link status signal units (indicating such things as alignment status, out of service, or processor out send mode). Level 2 - Fill-in signal units (used for alignment control during link recovery). This count is pegged in the link interface when a level 3 type signal unit is received. It is essentially a count of all SS7 traffic messages. It includes ECIS6 messages, SCCP messages, and network management messages. This count, along with MGMSUX, BYMSUR, and BYMSUX, provides a good measure of traffic flow on the link.
MGMSUX (SS7)	Message signal units transmitted. When a message signal unit is transmitted, this count is pegged in the link interface. Refer to the MGMSUR description.
MRBADRTG (Office)	Message signal units discarded due to routing data error (no routing data). This count is a cumulative total of all SS7 message signal units handled by the SCCP in the central processor.
MRSBCO7 (Office)	DCIS6 message rejected due to congestion. Direct signaling messages are transmitted on SS7 links using DCIS6 protocol. If the transmit buffer of the outgoing link is congested or the far-end of the link is sending processor congestion messages, the direct signaling message is discarded, this count is pegged in the central processor, and an unaccepted direct signal message is returned to the originator. See the MRSBCO6 description.
MRSNTO7 (Office)	DCIS6 message rejected due to no translation data. Direct signaling messages are transmitted on SS7 links using DCIS6 protocol. If the translation for a DCIS6 message fails, it is blocked. The message is discarded, this count is pegged in the central processor, and the unsuccessful direct signal message is returned to the originator.
MSG7LOOP (SS7)	SS7 messages "looped" in the network. Before an SS7 message is transmitted, a check is made for looping message. Looping usually occurs when: (1) The message is blocked at some other node and must be returned to this node to be sent to the origination. (2) The normal outgoing route is blocked and the message must be rerouted. If the outgoing link set for the message is a direct or combined link set containing the incoming link and the message is an unsuccessful direct signaling type, it is looping. This count is pegged and the message is not sent. If the incoming link is a C-link, a TFP or TCP response is returned on the incoming link.
MSINSIO (SS7 or Office)	Message signal units discarded due to invalid Service Indicator Byte. This measurement is also counted per office as the sum of this measurement for all SS7 links.
MSUDISC_ (SS7)	Messages removed due to link congestion. The SS7 discard strategy (for level 1, 2, or 3). The node first checks the priority of a message before transmitting it. The priority is contained in the service information field and is compared with the congestion state of the transmit buffer. Refer to the L7LCDIS_X measurement description. If the priority is less than the congestion level, the message is removed, the corresponding count pegs, and a return message may be sent. Priority 0 messages peg MSUDISCO, priority 1 pegs

	MSUDISC1, and priority 2 messages peg MSUDISC2. The return message is sent only if the received message is not a UDS type. If the message to be transmitted is a unit data type SCCP message, a UDS message is created and returned to the originator. If the priority of the message is equal to or greater than the congestion level, it is transmitted and this count is not pegged.
MSURMV (SS7)	Messages removed due to link congestion. The SS7 discard strategy for level 1, 2, or 3 is used. The node first checks the priority of a message before transmitting it. The priority is contained in the service information field and is compared with the congestion state of the transmit buffer. Refer to the L7LCDIS_X measurement description. If the priority is less than the congestion level, the message is removed, the MSURMV count pegs, and a return message may be sent. The return message is sent only if the received message is not a UDS type. If the message to be transmitted is a unit data type SCCP message, a UDS message is created and returned to the originator. If the priority of the message is equal to or greater than the congestion level, it is transmitted and this count is not pegged.
MSUSAMPL	Number of message signal units (MSU) sampled for link output delay.
NACR (SS7)	Negative acknowledgement "event" occurred. Upon receiving a negative acknowledgement, this count is pegged once for the first signal unit that must be queued for retransmissions and not again until the event ends. If subsequent signal units must be queued for retransmissions, this count is not pegged. Once sequencing is correct, the event has ended. The basic error correction method in SS7 involves both positive and negative acknowledgements. Each signal unit has a forward sequence number and indicator and a backward sequence number and indicator units header. The backward sequence number and indicator in a received signal unit is compared with the forward sequence number and indicator in a previously transmitted signal unit to determine whether a positive or negative acknowledgement is being indicated by the far-end. Each received signal unit normally positively acknowledges the previous transmitted signal unit. Any signal unit not positively acknowledged are queued for retransmissions. A positive acknowledgement received for any transmitted signal unit causes all previous transmitted signal units to be positively acknowledged along with any previously transmitted signal units.
NOCMG (Office)	The number of times the system entered a state in which it could not process CCS messages. The basis of this measurement is an internal timer which records the current time once each second as long as messages are being processed. When an inability to process messages is detected, the timer stops and a flag is set indicating "no message processing state." When the problem clears, the timer starts and the elapsed time is calculated. The flag is reset and this count is incremented.
NOCMGT (Office)	The accumulated time in seconds during which no messages could be processed. See the NOCMG measurement for a description.
NDCFLABN (SS7)	Number of signaling link declared failures due to abnormal conditions. This count is pegged in the central processor.
NDCFLHWP (SS7)	Number of signaling link declared failures due to general hardware problems. This count pegs in the central processor.
NDCFLSWP (SS7)	Number of signaling link declared failures due to general software problems. This count pegs in the central processor.
NDCFLXDA (SS7)	Number of signaling link declared failures due to excessive delay of acknowledgement. This count is pegged in the central processor.
NDCFLXDC (SS7)	Number of signaling link declared failures due to excessive congestion duration. This count pegs in the central processor.
NDCFLXER (SS7)	Number of signaling link declared failures due to excessive error rate. This count pegs in the central processor.
OCCUPMSU	Link transmission buffer average occupancy based on ten-second scans.
ORIGMSUS (SS7 or Office)	Originated message signal unit. This measurement is the number of message signal units transmitted by the node in which the originating address specifies this signaling point. One example of this type of message is a network test message. This measurement is also counter per office as the sum of this measurement for all SS7 signaling links.

ORMSUOCT (SS7 or Office)	Originated message signal unit bytes. Refer to ORIGMSUS count. The sum of this measurement for all SS7 links is also counted per office. This count is incremented by the length of the message signal unit bytes. The headers on messages counted by this measurement is eight bytes longer than the headers on messages counted in the link interface.
RABT (SS7)	Number of abort events received on the link. When an abort event, also called byte counting event, is indicated by receiving more than seven consecutive "1" bits, this count is pegged in the link interface. This condition is called by either hardware and/or software problems or 51 digital facility resynchronization.
RABTER (SS7)	Number of bytes received in error during abort events. Errors detected during abort events are included in the signal unit error rate monitor. This count is the cumulative total of these errors and is pegged in the link interface. The average burst size of facility failures in this count divided by the RABT count.
RTESETUN (Cluster)	Route set unavailable. The application uses a specific set of routes to send messages to a specific cluster of destinations. Availability of the route set is determined by the availability of the link set along with path to the cluster. Failure of any link set could result in one or more becoming inaccessible to this office. This count is pegged when a member of the indicated cluster becomes inaccessible due to route set unavailability. This count is the total number of times a member becomes inaccessible, but does not indicate current accessibility.
RTESETUNT (Cluster)	Duration of route set unavailable. This measurement is not the cumulative duration of each member's inaccessibility, but is the total time during which any member in the indicated cluster is inaccessible.
RTGAUDFL (Office)	Routing audit failure. This measurement is the total number of times the routing audit failed for any node in the office. See L7RTGAUD description.
SC7R (SS7)	Signaling connection control part message received. This is the total number of messages received by the SCCP in the node. These messages may be global title routed or point code routed and some may be sent to the central processor for handling. This count includes messages destined for this point code (the SC7RLNN count) or destined for some other point code not counted. It is pegged in the node when the message is received from the network.
SC7RERPRO (SS7)	An SCCP message destined for a prohibited subsystem. This measurement is the total number of messages received by SCCP in the node destined for a local or distant prohibited subsystem. The count is pegged in the node when the message is received from the network.
SC7RERUA (SS7)	An SCCP message destined for an unknown address or global title. This measurement is the total number of messages received by SCCP in the node destined for an unknown address or global title. The count is pegged in the node when the message is received from the network.
SC7RERUATY (SS7)	An SCCP message destined for an unknown address or global title type. The SCCP global title routed messages are destined for the central processor for global title translation. This measurement is the total messages received by SCCP in the node destined for an unknown address type. The count is pegged in the node when the message is received from the network.
SC7RERUNE (SS7)	An SCCP message destined for an unequipped subsystem. This measurement is the total messages received by SCCP in the node destined for an unequipped subsystem. The count is pegged in the node when the message is received from the network.
SC7GTR (SS7)	An SCCP message destined for global title routing. This measurement is the total number of messages received by SCCP in the node using global title routing (such as DCIS6 messages). A global title is either a function number or an NP-NXX. The count is pegged in the node when the message is received from the network.
SC7LNN (SS7)	An SCCP message destined for the local network node. This measurement is the total number of messages received by SCCP in the node destined for this point code. The count is pegged in the node when the message is received from the network.
SC7RLSS (SS7)	An SCCP message destined for an equipped local subsystem. This is the total number of messages received by SCCP in the node destined for a point code that is a subsystem at this location. It is pegged in the node when the message is received from the network.

SC7NATL (SS7)	Messages discarded due to blocked point code. When any message destined for an inaccessible signaling point is received, it is discarded and this count is pegged in the incoming node. This count is cumulative for all point codes.
SC7UDSX (SS7)	Unit data service message transmitted in response to a unit data message type failure. When a unit data message is received by SCCP, a unit data service message may be sent to the originator. If SCCP cannot deliver a message to its destination for one of the defined unit data service reasons and the message indicated a unit data service message should be returned, the unit data service message is formatted and returned to the originator. This count is pegged in the node when the unit data service message is sent.
SCR (Office)	An SCCP message received. This measurement is the total messages received by SCCP in the central processor. These messages may be global title routed or point code routed. This count includes messages destined for this point code or destined for some other point code. It is pegged when the message is received by the central processor.
SCRERPRO (Office)	An SCCP message destined for a prohibited subsystem. The prohibited subsystem may be either local or distant. This measurement is the total number of locally originated SCCP messages received by message handling in the central processor destined for a prohibited subsystem. The count is pegged when the message is received by message handling in the central processor.
SCRERUA (Office)	An SCCP message destined for an unknown address. A locally originated SCCP global title routed message can be translated to a destination point code (called global title translation). Should the application be unable to translate the global title in the received message, this count is pegged and the unit data service message may be returned. This count is not to be confused with the SCRERUATY measurement. This count indicates the number of messages that failed global title translation due to no translation data. The latter is a count of messages received for translation of a global title type that is not provided.
SCRERUATY (Office)	An SCCP message destined for an unknown address type. Should the application not provide a capability to translate the global title type in the received message, the message handler pegs this count. The count is the total number of locally originated SCCP messages received by message handling in a central processor that are destined for global title translation of an unknown (or unprovided) address type.
SCRERUNE (Office)	An SCCP message destined for an unequipped subsystem. This measurement is the total locally originated SCCP messages received by message handling in the central processor destined for an unequipped subsystem. The count is pegged when the message is received by message handling in the central processor.
SCRGTR (Office)	An SCCP message destined for global title routing. This measurement is the total number of messages received by the SCCP in the central processor using global title routing. A global title is either a function number or an NPA-NXX. The count is pegged when the message is received by message handling in the central processor.
SCRLNN (Office)	An SCCP message destined for the local network node. This measurement is the total number of messages received by SCCP in the central processor destined for this point code. The count is pegged when the message is received by message handling.
SCRLSS (Office)	An SCCP message destined for an equipped local subsystem. This measurement is the total locally originated SCCP messages received by message handling in the central processor which is destined for a local subsystem that is equipped. The count is pegged when the message is distributed by message handling in the central processor.
SCSRTR (Office)	Subsystem routing test message received. This measurement is the total test messages received by the SCCP. When the message is received by the central processor, this count is pegged.
SCSRTX (Office)	Subsystem routing test message transmitted. This measurement is the total of such messages transmitted by the SCCP. When the message is sent by the central processor, this count is pegged.
SCSSTR (Office)	Subsystem status test message received. This measurement is the total of such messages received by the SCCP. When the message is received by the central processor, this count is pegged.
SCSSTX (Office)	Subsystem status test message transmitted. This measurement is the total of such

	messages transmitted by the SCCP. When the message is sent by the central processor, this count is pegged.
SCUDSX (Office)	A unit data service message is transmitted in response to a unit data message type failure. When a locally originated unit data message is received by message handling in the central processor, a unit data service message may be sent to the originator. If the SCCP cannot deliver the message to its destination for one of the defined unit data service reasons, and the message indicates a unit data service message should be returned, the unit data service message is formatted and returned to the originator. This count is pegged when the unit data service message is sent by message handling in the central processor.
SEVERSEC (SS7)	Severe error seconds. This count is the total number of seconds during which the link had more than 64 errors. It is pegged in the link interface and can be used to monitor and characterize T1 facility failures.
SPI (SS7)	Adjacent signaling point isolated due to local failure. A link set along a path to the indicated destination failed causing a complete failure of all signaling paths to the destination. Failure of any signaling path caused by either a local link set failing or the receipt of a transmission failure message indicating some link set along the path to the destination failed. Refer to the SPIA, SPIB, and SPIC descriptions.
SPIA (Office)	Adjacent signaling point isolation due to local failure of A-link. This condition occurs when all C-links are unavailable, and the last A-link to the indicated destination fails or receives a transmission failure message indicating some link set along a path to the destination failed. This is a cumulative total of the SPI count for all A-links in the office.
SPIAT (office)	Duration of SPIA.
SPIPO (SS7)	Adjacent signaling point isolation due to far-end processor outage. A link failed due to receiving a processor message from the far-end causing a complete failure of all signaling paths to the indicated destination from this office. The effect is the same as the SPI due to local failure.
SPIPOT (SS7)	Duration of the SPIPO measurement. This time period begins when the local link fails due to receiving the processor outage message. It ends when any link set along a path to the destination restores. The count is the total time the far-end is isolated from this office.
SPISP (Office)	Adjacent signaling point isolated due to local failure. This is a cumulative count of all SPIs for all links in the office.
SPISPT (Office)	Duration of SPI measurement. This count is the cumulative duration of all SPIs for all links in the office.
SPIT (SS7)	This time period begins when a link set along a path to the indicated destination fails causing it to be isolated. It ends when any link set along a path to the destination restores. The count is the total time the far-end is isolated from this office.
SQL (SS7)	Link quality. A relative measure indicating the percentage of time the link is operated without errors. This measurement is derived from the ERSEC count.
TDPRCNGO	Cumulative duration of processor congested state.
THRSWMSU (SS7 or Office)	Through-switched message signal units. This measurement is the number of message signal units received by the node in which the destination address does not specify this signaling point. This measurement includes most nonglobal title rerouted messages and should be very close to the MSURECVD count. This measurement is also counted per office as the sum of this measurement for all SS7 links.
TLNKACTION (SS7)	Signaling link active time. This time starts when the link restores to service and stops when the link fails or is moved to maintenance-out-of-service state. The count pegs in the central processor.
TPROCOTG	Cumulative duration of processor outage.
TRMDMSUS (SS7 or Office)	Terminated message signal units. This measurement is the number of message signal units received by the node in which the destination address specifies the signaling point. One example of this type of message is global title translation. This measurement is also counted per office as the sum of this measurement for all SS7 links.
TRMSUOCT (SS7 or Office)	Terminated message signal unit bytes. Refer to TRMDMSUS measurement. This measurement is also counted per office as the sum of this measurement for all SS7 links. This count is incremented by the length of the message signal unit in bytes. The headers on messages counted by this measurement are eight bytes longer than the

	header on messages counted in the link interface.
TSMSUOCT (SS7 or Office)	Through-switched message signal unit bytes. Refer to the THRSWMSU measurement. This measurement is also counted per office as the sum of this measurement for all SS7 links. This count is incremented by the length of the message signal unit in bytes. The headers on message counted by this measurement are eight bytes longer than the headers on messages counted in the link interface.
UNVL (SS7)	Link unavailable. A relative measure indicating the percentage of time the link is out of service.
ZPEAKOCC	Link transmission buffer peak occupancy based on ten-second scans.

3.13.2 Description Of Reports

3.13.2.1 Fixed and Flexible Format Reports

The measurement reports may present the data in either a fixed or a flexible format. There are two ways to view the measurement data. The reports present a specific view of the common measurement data and some reports make this view definable via a measurement output control table. Automatic reports are output as REPT SMR messages, while demand reports are output as OP SMR messages. The reports are available in two formats as follows:

- (1) **Fixed format reports** - Certain measurement data is provided in a fixed layout. This data is output automatically and on demand.
- (2) **Flexible format reports** - This format allows the user to have any specified set of measurement data output in one of four ways. These can be scheduled or on demand.

Following the general discussion of the various report types are some examples of each of the fixed format reports.

3.13.2.2 Report Data

The data in a report is derived from the measurements found in the history files or the latest period measurements. The data in the report is used to evaluate the performance of the CNI-equipped office and the SS7 network. The measurements provide details needed to identify equipment and signaling performance faults. Different reports contain different measurements. The measurement data on any particular report type is defined by the specific column and row heading shown.

All report types contain a common header section which provides the following:

- Identifying information for the reporting office (such as, software release and CLLI code)
- Identifying information for the particular report being output (such as, the report name, time, report coverage, and whether or not it is being generated automatically).

Since some of the measurements in the history file are on a per-link or per-node basis, sometimes the measurements must be accumulated during the generating process to derive a useful value for outputting to users. The final values provided depend on how the data is accumulated. Ring node out-of-service counts may be cumulated on the basis of protocol, or on the basis of the type of node they serve. The same measurement data is used in both cases, but is shown differently for different uses. Since the per-office measurements may include the same counts as the per-link or per-node measurements, each piece of data is known by a different name. The scope of a particular piece of measurement data is referred to as "granularity." The granularity of the count determines the report in which the data is useful.

To provide information in a more usable form, some data values shown in a report may be the sum of several measurements. In the report examples shown in this part, the basic measurement used to derive the value is shown. Where the value is not obtained from the history file, no name is given. The names shown do not appear in the report and are not strict definitions of each value. They are included to help the reader understand the source of the data for use in cross-referencing the report to the measurement tables shown earlier.

Measurements take three forms as follows:

- Peg counts (indicated by a PC in the report)
- Time durations (in hours, minutes, or seconds)

- Thresholds (indicated by a TE in the report).

Most reports contain more than one of these forms. A peg count, for instance, may also contain the corresponding duration on the same report line. In the illustration of the report layout, the measurement name is shown just once and when more than one term is shown, an underscore (_) is shown in place of the suffix.

In some unusual circumstances, the data in a report may be incomplete. This is possible if a node is out of service or a fault occurs during measurement collection. Some reports flag invalid data, and other reports indicate when the data is questionable. In reports with specific link data (such as, SNPR2 and 30MPR reports), an asterisk appears in the link type field if there is no data available for the link.

3.13.2.3 Network Clock

Centralized support systems control and administer the CCS network. The CNI generates reports and CCS network critical event messages for these support systems. The information provided by the CNI reports and critical event messages gives the support systems information for determining the condition of the various nodes in the network. A network clock provides the uniform time stamping of the reports and messages to maintain synchronization in general. The network clock uses the *UNIX*® system RTR internal clock in each node and various control functions between nodes to maintain a single time reference throughout the network. Showing report periods in network time provides this single time reference for support system users. A user may check the validity of the network time by using the `OP-SNAT` or `REPT:SNAT` message.

Two network nodes are designated as the master/mate clock pair to provide the network time to all other nodes in the network. The node that is currently the master is responsible for notifying all other nodes of the correct network time. When initialization of the master node, the time is set manually using a standard reference. The purpose of the mate clock node is to act as master should the current master node fail. The `FORCED SWITCH` message is broadcast to all offices whenever the mate is redesignated as the master node. All offices then expect and receive the proper network time from the newly designated master node. The input message `SW:CLOCK` provides a means to manually initiate a forced switch.

When all nodes are functioning properly, the master node periodically broadcasts a `TIME` message to all other CNI-equipped offices including the mate clock node. Each CNI-equipped office, in turn, responds by broadcasting the time message to all end offices. When an office receives the `TIME` message, it updates the *UNIX*® system RTR clock and reports any deviations to users via the `REPT CMMSSADM` output message. If an office has time deviations exceeding some predefined limit, it queries the master node to maintain synchronization.

If an office fails and recovers, it must query the current master node for the correct network time. The `TIME` message sent to the requesting office in response to a query is used to update the internal clock in the receiving office for generating the deviations report. When a `TIME` message response is not received in response to a query, the node queries the master a maximum of three times before notifying the user to manually set the *UNIX*® system RTR clock. The `REPT CMMSSADM` message notifies users of both normal and abnormal network clock operation.

3.13.2.4 Reports and Measurement Data Output

The users of the measurement data are involved in daily maintenance and operations of the CNI-equipped office from various support system centers. All measurement data gathered is available to any of the users via the output control features of the measurement output control table. When IMS measurements are inhibited, however, some measurements are not available. To determine if the IMS measurements are inhibited, enter `INH:IMSMEAS STATUS!`.

In addition to the scheduled printing of fixed format reports, they can be obtained any time with the `OP:SMR` input message. This output request message causes the system to search the measurement output control table schedule for the report specified. When the entry is found, the report is generated and printed using the current

data found in the appropriate history file. Most scheduled and demand reports appear on the receive-only maintenance printer.

Since the measurement output control table provides for a delay of up to 5 minutes, the scheduled report may not be printed at the precise scheduled time. This delay is to prevent pages of different reports scheduled to print at the same time from being intermingled. Some reports may be specified as *polled* reports which are not output at all, but rather are generated and stored for later retrieval.

NOTE: The system is usually busiest at 15-minute intervals updating history files and printing scheduled reports. Demand reports should be requested at 5- to 10-minute periods after the 15-minute intervals.

Measurement data can be demanded on an individual measurement basis at any time. Individual measurement messages provide more current real-time data than reports. These are most useful to office personnel when troubleshooting. To request specific measurements, use the `DUMP:SMEAS` message. This command can provide specific measurements for specified links, nodes, etc., or it can print data on all links, nodes, etc. The measurement data is retrieved from the history files and output according to the measurement type. The data is sent to the requested designation as an output message. This command is available for on-site users to obtain more detailed measurements of conditions identified, but it is not available to support system users.

Support system users receive measurement data from the CNI-equipped offices via BX.25 data links. Reports and messages are sent to the support system via different BX.25 data links. Reports designated as polled are saved in specific files in a standard system directory. Support system users and on-site users may request data from these files with the `DUMP:SFILE` message.

3.13.2.5 Report Formats

3.13.2.5.1 Flexible Reports

The report names found in the measurement output control table are indicative of the format and the frequency of the output, the source history file, and the scheduled/demand aspect of the report. The report names are specified by a centralized administrative organization. Refer to the measurement output control table office record for this information.

The user can specify their own flexible reports via the measurement output control table. The measurement output control table controls the following:

- What data goes into the report
- When the report is output.

The flexible format reports are:

- CMNFDISK — Non-fixed Regular (prints all values) from Disk. Use 6 for this value.
- CMNFDISKEX — Non-fixed Exception (prints only where thresholds are exceeded) from Disk. RC/V view 15.6 (EXCP table) must be filled out to use this report.
- CMNFLPM — Non-fixed Regular (prints all values) from Last Period Measurement(LPM). Use 8 for this value.
- CMNFLPMEX — Non-fixed Exception (prints only where thresholds are exceeded) from Last Period Measurement (LPM). RC/V view 15.6 (EXCP table) must be filled out to use this report.

The user wishing to take advantage of Flexible Reports has to use CNI RC/V to create Measurement Output Control Table (MOCT) information. This procedure is described in the following text.

- (1) Access screen 15.5 (UVDI) in insert mode. Define the View Name, field 1, `user_defined_name`. Then fill the data fields with the desired measurement IDs. These IDs must be in ascending order (this is no longer required, but it is recommended). A list of measurement IDs and their numeric translations are supplied in 235-118-213, *Recent Change Manual*.
- (2) If the user wants measurement counts suppressed unless certain thresholds are exceeded then screen 15.6 must be accessed and the thresholds assigned to the previously mentioned measurement IDs.
- (3) Do not modify the History File Descriptor Table (RC/V 15.7, HFDT). Use the default values as provided.
- (4) Fill out screen 15.8 (Schedule) as follows:
 - **Field 01** — Enter `user_defined_report` name. For custom reports, this name must have one of the following formats:
 - If field 10 is 0 (poll), the format must be `AAAAXXXX`, where A is any alpha value and X is X.
 - If field 10 is 1 (auto), then the format can be `AAAAAAA`, where A is any alpha value.
 - If field 10 is 2 (poll/auto), then the format must be `AAAAXXXX`, where A is any alpha value and X is X.

On output of the report, the system will replace the `XXXX` with a time stamp. For example, if system time for the report is 04:20:00 to 04:25:00, the time stamp will be 0420 for the start of the report period.

- **Field 02** — Enter destination. Destination must be a value listed in an ECD classdef form. For example, the normal spooler classdef form "102" which lists `rop0`, `ttya` and `ttyz`.
- **Field 03** — Enter 06 for CMNFDISK.

Enter 07 for CMNFDISKEX.

Enter 08 for CMNFLPM.

Enter 09 for CMNFLPMEX.
- **Field 04** — Blank for this application.
- **Field 05** — Enter view name defined in Step 1.
- **Field 06** — Enter history file, most likely LPM.
- **Field 07** — Enter activation time, the time at which the user wishes the reports to start for each day's activities.
- **Field 08** — Enter REPEAT value.

Automatic	→	-1.
Demand	→	0.

A value > 0 means how many times output will be repeated starting at activation time. Since there are 288 five minute periods in one day, if the user enters 288 [if start time is midnight] the report will be output every five minutes. If the user enters 12, the report will be output every 12 "five minute periods," in other words, once an hour. In general, you will get your report every X five minute periods, where X is a number from 1 to 288. We recommend that the user set activation time to midnight [0000] if 24 hour

report coverage is desired.

- *Field 09* — Enter 1 or 0 for 'print if empty' decision. If 0, no report will be output if it's empty. If 1, report will be output regardless.
- *Field 10* — Enter 0, 1, 2. 0 → poll: sent to a file. 1 → auto: sent to a spooler output class(output to specified destination) 2 → both of the above.
- *Field 11* — Enter value [in seconds, MAX==300] for print delay.

If the user at this point does an `OP: SCHD (OP: SCHD, DEST=1` for ROP) the new custom report will now be listed on the screen and at the ROP with all the other reports. It will be available on demand or automatically as defined by the user.

(5) Exit CNI RC/V.

(6) To demand the report enter this command: `OP: SMR=CUSTXXXX, DEST=1`, where `CUSTXXXX` == the `User_defined_report_name`.

Because these custom reports are dynamic and NOT pre-defined, there is only rudimentary formatting of the data.

3.13.2.5.2 Fixed Format

A fixed format report contains a fixed set of measurements and the contents cannot be changed. The view in the measurement output control table with a fixed format report should not be changed. The data is presented with labels arranged in a fixed layout.

The format names are forms of the names used to specify a particular report. All reports fall into one of three categories as follows:

Total Office: Total office reports provide a general view of the office. The data in the reports is a summary of office performance. There are two total office fixed format reports as follows:

- (1) Signaling Network Performance Report, Part 1 (SNPR1)
- (2) Machine Performance Report (MPR).

The SNPR1 and the MPR are scheduled to be output daily and hourly. Therefore, they should be output on site every hour.

Detailed Performance: The detailed performance reports provide a closer look at the individual links and nodes. There are separate measurements for each link in the office. Thus, the reports provide information helpful in isolating problems to a particular link or node. They are necessary for compiling monthly performance reports. There are three detailed performance reports as follows:

- (1) Signaling Network Performance Report, Part 2 (SNPR2)
- (2) Signaling Equipment Performance Report (SEPR).
- (3) Signaling link 15-Minute Machine Resource Performance Report (ZMMPR).

The SNPR2 and SEPR are quite lengthy. Therefore, they are scheduled to be output only once each day and only on site.

Exception: Exception reports are used to single out those measurements that are significant when they exceed some predetermined value. Any measurement in an exception report that does not exceed this predetermined value is not output in the report. If there are no measurements that exceed their respective thresholds, the report itself may not be output. The report shows specific pieces of equipment that have experienced higher than normal errors or excessive loading. There are two fixed format exception reports as follows:

- (1) Thirty-Minute Marginal Performance Report (30MPR)
- (2) Ring Peripheral Controller Overflow Report (RINGX).

Both reports, output on site, identify problems with either signaling links or ring peripheral controllers, respectively.

3.13.2.5.3 Flexible Format

Flexible format reports are user-defined. The CNI allows the user to create customized reports containing data pertaining to their needs via the measurement output control table. These reports require a view in the measurement output control table to specify what measurements should be printed. The view is used to extract measurements from the data base.

When users in the support centers need reports for a specific purpose and the desired information is not available in a fixed format report, or the fixed report is not available, a new report can be created to fit the need. To generate this report, use the measurement output control table to specify the name, content, frequency, and format of the desired report. You can also specify if the report will be output automatically or only on demand. The format is specified by using the appropriate flexible format report generator.

Flexible format reports can be either regular or exception reports. The regular format shows a value for all measurements specified in the view regardless of value. The exception format shows a value for all measurements specified if any one of those measurements has exceeded its threshold. The report header information and additional report parts are as follows:

- Report header information:
 - Report name
 - Day of year (1 through 366)
 - Number of 5-minute intervals at measurement start time
- Per-office measurements
- Per-link measurements
- Per-node measurements
- Per-channel measurements
- Per-cluster measurements.

Each report appears as follows:

aaa =	Number of measurements in this part List of measurement names
bbb =	Identification of link, node, channel, cluster, or link set Corresponding values

ccc = Identification of next link, node, channel, cluster or link set Corresponding values

NOTE: If a report is scheduled near midnight and is output the following day, the header may show the past day. The report reflects when the data was created rather than when the report is output.

Normally, flexible format reports are sent to users at support centers. The report generated is little more than a list of measurement values to be sent to the support system over dedicated data links. The user at the support center then formats the data further.

3.13.2.6 Signaling Network Performance Report, Part 1

The SNPR1 is a total office report that is output automatically for each hour and once for the entire day. The purpose of the report is to provide an overall view of signaling performance for the office.

The report does not provide detailed measurements for each link. Therefore, the data on this report cannot be directly used to determine the condition of any specific piece of hardware. It shows cumulative counts for the entire office. The area reflected in this report are signaling load handled, signaling link failures experienced, signal unit errors detected, and the number of message transfer failures that occurred.

This report should be checked daily for counts indicating poor link performance. The hourly reports from any period should be compared for trends and abnormalities. Keep in mind that a high count on one report does not necessarily indicate problems. The same counts occurring at the same time each day may point to externally induced problems. If problems are indicated, refer to the Signaling Network Performance Report, Part 2 (SNPR2) or the Thirty-Minute Marginal Performance Report for detailed measurements of specific links. The counts of particular concern are as follows:

- Emergency Restarts (EMR)
- Signal Unit Errors (SUER_TE)
- Retransmission Requests (SUERX_TE)
- Repeated and Skipped ACUs (AURSTE).

Two sections in this report are as follows:

- Header information
- SS7 link data.

Each link data section contains signaling load measurements and signaling performance measurements.

3.13.2.6.1 Header Information

The header information provides the following:

- Office identification
- Report type
- Time
- Data coverage.

3.13.2.6.2 SS7 Signaling Load and Signaling Performance Measurements

The SS7 signaling load and signaling performance measurements identify the number of messages received and transmitted for various SS7 message types and various failure conditions for SS7 links. They include counts and exception threshold measurements for certain error conditions that indicate poor link performance. Also shown are the following:

- Message counts [embedded common channel interoffice signaling (ECIS) and direct common channel interoffice signaling #6 (DCIS6)] discarded because of blockage or translation failure
- Counts of looping messages
- The number of routing audit failures
- Global title translation counts.
- Counts of traffic diversion to lower priority link sets.
- Counts of traffic diversion to lower priority link sets, other than C-link sets.

Points to consider when interpreting the measurements are:

- Byte and signal unit load counts are pegged in the link interface. They do not include SYNC, ACU, or PRO messages. They do include signal units received in error.
- Message counts are pegged in the node. They include messages that may subsequently be blocked at the outgoing node.
- The embedded CCIS6 (ECIS) protocol signaling load measurements count all CCIS6 messages that are sent or received on CCIS7 virtual links. Furthermore, the count of SS7 routed messages includes the ECIS type.
- Signaling point isolation indicates failure of all signaling paths to an adjacent signaling point. A signaling path failure is indicated by local link failure, far-end processor outage, or receipt of trunk failure messages indicating some link in a path to the destination has failed.
- Discarding messages because of link congestion is related to the transmit buffer occupancy and the priority of the message to be transmitted. If the priority level is less than the congestion level, the message is discarded. Depending on several factors, a return message may be sent indicating the reason for discard.
- Level 1 congestion is the lowest congestion state for the link. Duration measurement for this state shows how long buffer occupancy is above normal. The peg count indicates how often occupancy is above normal, but not how serious the congestion is.
- Errored seconds are the number of 1-second intervals during which signal units were received with errors. It is not a count of signal unit errors. Detected errors indicate the number of signal units that failed the parity check. An excess of these could cause the link to be declared failed.
- Looping messages are usually caused by congestion or blockage at an outgoing link combined with messages returned from some far-end office. When looping counts are high, look for other counts indicating congestion, blockage, no translation, and possibly discarded messages.

3.13.2.7 Signaling Network Performance Report, Part 2

The SNPR2 is a detailed report of signaling link performance. It is output automatically once each day. The

purpose of the report is to provide enough detail on each signaling link in the office to allow troubleshooting of faulty links and the compilation of statistical data on each link. The report consists of a number of pages because of the amount of data provided. Each page of the report is output as a single message.

The SNPR2 report and the Thirty-Minute Marginal Performance report are the main sources for analyzing link failures and marginal performance. The SNPR2 provides an overview of signaling capabilities for the office giving a detailed description of SS7 link performance. This report should be checked whenever link problems are indicated. The counts in the SS7 link performance section are of particular concern since the data is mostly an expansion of similar total office data provided on the SNPR1 report. The SNPR2 reports should be compared each day to determine trends in signaling link problems and provide long-term analysis intermittent problems.

The link performance section of the SNPR2 report provides data for each equipped link (provided all measurements on the particular report line in question are other than zero). If there is no data available for a link, the type field is shown with an asterisk. The measurements for each link are listed on separate lines with link identification (CLLI code, layer number, link type, group number, and member number) to the left of each. The three sections of the report are as follows:

- Header information
- Loss of signaling capability
- SS7 link performance.

3.13.2.7.1 Header Information

The header information section provides office identification, report type, time, and data coverage. In addition, this section shows the number of equipped links in the office and the combined active time for all links.

3.13.2.7.2 Loss of Signaling Capability

The loss of signaling capability section indicates how often (and how long) particular categories of links were unable to provide signaling. The degree that signaling can be impaired is identified as follows:

- The emergency restart shows a loss of signaling (banded or ECIS) to an adjacent office. The data is cumulative for all SS7 links.
- A signaling point isolation indicates loss of signaling to an adjacent office. The count that pegs this is the signaling point isolation count for link type of the last link to fail causing the isolation.
- A link set failure indicates alternate routing is necessary to the far-end office and all affected destinations. If the link set failure results in failure of the combined link set, the far-end becomes isolated.

3.13.2.7.3 SS7 Signaling Link Performance

The SS7 signaling link performance section provides the most important measurements for analyzing SS7 link performance. These are grouped as follows:

- Failed time, errored seconds, detected signal unit errors, and bytes transmitted
- Automatic changeovers, declared failures, and link set failures
- Signaling point isolations, discarded message signal units, and transmit buffer congestion
- Duration (in seconds) that traffic is diverted to a lower priority link set, number of times that traffic is diverted to

a lower priority link set

- Duration (in seconds) that traffic is diverted to a lower priority link set, not including the C-link set; number of times that traffic is diverted to a lower priority link set
- Emergency restarts.

Refer to the SS7 performance description of the SNPR1 report for important points to consider when analyzing the SS7 signaling link performance measurements.

3.13.2.8 Signaling Equipment Performance Report

The SEPR is a detailed report on node performance that is output once each day. The purpose of the report is to provide a profile of each node's status for the reporting period.

The report should be examined to note any excessive counts. The OOSAU_ (automatic out-of-service counts and durations) and OOSCFG_ (reconfigured out-of-service counts and duration) columns of the report are of particular concern. This is especially true in the ring peripheral controller node section. Proper operation of the ring peripheral controller is critical to the message switching function.

Any node out of service may be caused by node processor or ring interface problems. Problems in the link node may be caused by poor link performance. When a link is declared failed, the node is automatically removed from service to perform diagnostics. A normal link is not necessarily declared failed when the node is removed because of other problems. The ring peripheral controller node (RPCN) problems may be caused by the dual signal channel problems. The report may indicate problems in a specific node or the ring in general.

The SEPR report does not provide a detailed analysis of why a node failed. The out-of-service counts and durations are provided for each node according to the major cause of the change to out of service or standby state. The following are three conditions that may cause this report to be generated:

- Automatic action because of a node or link fault
- Manual action
- Ring reconfiguration affecting a normally operating node.

A total count of the number of times a node restarted for any reason is provided. A few points to consider for interpreting the report are as follows:

- The duration counts are cumulative for all occurrences.
- The out-of-service counts indicate the *initial* reason for a node being removed. The node maintenance state may change without affecting the out-of-service measurements as long as the major state remains the same. For example, a node removed because of failing diagnostics causes the out-of-service automatic count to peg. Later changing the node state to manual out of service (MOOS) does not cause the out-of-service manual count to peg.

The data is provided, one node per line, with group and member number identification to the left. If a node is not in the out-of-service state at any time during the reporting period, it is not shown in the report. There are five sections to the report as follows:

- Header information
- SS7 link node performance

- Special access data channel (SADC) link node performance
- D-channel link node performance
- Ring peripheral controller node performance.

3.13.2.9 Machine Performance Report

The machine performance report is a total office report that is output automatically for each hour and once for the entire day. The time of the report is important when isolating problems. The purpose of the report is to provide an overall view of the message switching capability for the office.

The report does not provide detailed measurements for each link or node. The machine performance report shows cumulative counts for the entire office. This report can be used to determine the message switching status of the office in general.

The report should be checked daily for counts indicating ring node failures or degraded ring performance. The hourly reports from several measurement periods should be compared for trends and abnormalities. A high count on one report does not necessarily indicate a problem. The same counts occurring at the same time each day may point to externally induced problems. If problems are indicated, refer to the signaling equipment performance report or ring exception report for detailed measurements of specific nodes.

There are several sections to this report as follows:

- Header information
- System identification
- No message signal unit processing
- Ring peripheral controller node performance
- Link node performance
- Ring performance
- Internal congestion.

3.13.2.9.1 Header Information

The header information provides the following:

- Office identification
- Report type
- Time
- Data coverage.

3.13.2.9.2 System Initialization

The system initialization section shows how many times specific levels occurred (and for how long) for each

system. Since initialization of each subsystem is triggered by a higher level subsystem (for example, the application starts the CNI initialization and the CNI starts the IMS), the counts for a particular level are normally the same for all subsystems. A few points to consider when interpreting the measurements in this part of the report are as follows:

- A *UNIX*[®] RTR operating system or application level 1 leads to either a 1A or 1B IMS level (there is no level 1 in the IMS initialization). The message switch is stopped by the level 1B but not by the level 1A.
- Levels 0, 1, 1A, or 1B do not include a boot.
- The *UNIX*[®] RTR system operating 5x levels generally correspond to the application x levels.

A brief description of each initialization level is:

- 0 - **Audit level:** No interruption of message switching.
- 1 - **Recovery level:** Process communication and data tables are reinitialized. No processes are recreated, but some messages may be lost.
- 3 - **Lowest boot level:** All processes are recreated and RPCs are pumped.
- 4 - **Highest boot level:** All processes are recreated and all nodes are pumped.

3.13.2.9.3 No Message Signal Unit Processing

The "no message signal unit performance" part of the report shows how many times the CNI entered a state in which it could not process CCS messages. This should be, at least, the sum of the IMS levels 1B, 3, and 4 initialization; although the state could occur without initialization.

3.13.2.9.4 RPCN Performance

The RPCN performance part of the report provides out-of-service counts and durations for ring peripheral controllers, in general, according to the major cause of the change to the out-of-service or standby state. The following are three conditions that may cause this report to be generated:

- Automatic action because of a node or link fault
- Manual action
- Ring reconfiguration affecting a normally operating node.

A cumulative count of the number of times any node restarted for any reason is provided. The data provided in this part of the report is similar to the per-node data in the signaling equipment performance report.

3.13.2.10 Signaling Link 15-Minute Machine Resource Performance Report (A15MPR15)

The fifteen-minute machine resource performance report is a detailed report of SS7 signaling link performance. If scheduled, it can be automatically output every 15 minutes. The purpose of the report is to identify loadsharing problems. This report should be checked when link problems are suspected.

There are two sections to this report:

- Header information
- SS7 links

3.13.2.10.1 Header Information

The header information provides:

- Office identification
- Report type
- Time
- Data coverage.

3.13.2.10.2 SS7 Links

The SS7 links part of the report provides the following group of measurements:

- Count of signaling units received by on a link
- Count of signaling units transmitted by on a link
- Count of bytes received over a link
- Count of bytes transmitted over a link
- Count of declared link failures on a link

3.13.2.11 Thirty-Minute Marginal Performance Report (A30MPR30)

The thirty-minute marginal performance report is a detailed exception report of signaling link performance. It can be automatically output each 30 minutes, but only if one of the measurements contained in the report exceeds some predefined threshold. The purpose of the report is to identify links that are showing marginal performance. The set of measurements provided indicate various problems with the link; such as, parity errors in the received signal units, alignment problems, excessive changeovers, or excessive downtime.

This report should be checked when link problems are indicated. The thirty-minute reports of various measurement periods can be compared to identify trends and abnormalities. Look for failures associated with an individual link, group links, or a particular far-end office.

If any measurement in a particular section exceeds its threshold as specified in the measurement output control table, all equipped links in the section are printed. Those measurements that exceed their threshold are identified by an asterisk. If no measurements in a section exceed their threshold, the section is not printed. The number of pages to the report depends on the number of links that are included.

There are three sections to this report:

- Header information
- SS7 links
- SS7 clusters.

3.13.2.11.1 Header Information

The header information provides:

- Office identification
- Report type
- Time
- Data coverage.

3.13.2.11.2 SS7 Links

The SS7 links part of the report provides the following group of measurements:

- Total out-of-service time
- Count of signal units received with parity errors
- Count of bytes retransmitted
- Number of automatic changeovers initiated from the link.

Some points to consider when interpreting these measurements:

- Errored seconds in the number of 1-second intervals during which signal units were received with errors. It is not a count of signal unit errors. An excess of detected errors could cause the link to be declared failed.
- Since changeover/changeback sequence on a SS7 link involves extensive data retrieval, a longer link downtime may result.

3.13.2.11.3 SS7 Clusters

The SS7 cluster section shows peg counts and durations for each equipped cluster (local and remote). The counts indicate the CN1 office is unable to route messages to any destination in the indicated cluster. Note that the corresponding link set failure count pegs when a route set becomes unavailable.

3.13.2.12 Five-Minute Ring Exception Report

The five-minute ring exception report contains exception ring peripheral controller congestion status. It can be output automatically every 5 minutes, but will only be output if one of the measurements contained in the report exceeds some predefined threshold. If no measurements exceed their thresholds, the message `NO RPC OVERFLOW ENCOUNTERED` is printed out.

The purpose of the report is to identify ring peripheral controller nodes that are experiencing various levels of congestion. This report should be used with the machine performance report to determine possible causes of the congestion and appropriate action necessary to relieve it. Give particular attention to overflow levels 2 and 3 (RRBOVFLW2_ and RRBOBFLW3_).

There are two sections to this report:

- Header information
- Details of congestion status.

The header information includes:

- Office identification
- Report type
- Time
- Data coverage.

Congestion of the RPCN ring receive buffers indicates messages are being sent to the RPCN faster than it can process them. The report shows peg counts for levels 0, 1, 2, and 3, and duration counts for levels 1, 2, and 3. All link nodes are notified of their home RPCNs congestion status. A few points to consider when interpreting the measurements are:

- Level 0 is the normal discard state. Messages are discarded at higher levels.
- The peg count shows how many times the buffer occupancy reached the indicated level.

3.14 USER CONTROLLED PROTOCOL PARAMETERS

Certain timer values and congestion thresholds used by SS7 associated software are user adjustable. These timers and thresholds are called protocol parameters. These parameters are used by the signaling system to control link operation during normal and failure conditions. The network file is an American Standard Code for Information Interchange (ASCII) data file to provide the user the ability to establish the parameter values. The CNI reads the parameter values from this file during any level 4 initialization. The network file contains the network indicator and initialization instructions for all of the user controllable parameters.

Each controllable parameter falls into one of the following categories:

OFFICE-DEPENDENT — These parameters, listed in Table 3.14-1, have one value for the entire office.

LINKSET-DEPENDENT — These parameters, listed in Table 3.14-2, have a different value for each linkset in the office. In the network file, each linkset-dependent parameter must have either a linkset number indicating to which linkset the value applies, or the word `ALL` to indicate the value applies to all link sets. The CNI supports the international feature which has two types of parameters within the linkset-dependent group. The first type is referred to as normal parameters and has a default value that is the same for all linkset numbers. The second type is a different parameter, since they have different default values for international versus domestic linksets. This allows network file entries that specify an initialization value to be used for a particular linkset, all international linksets, all domestic linksets, or all linksets (international and domestic).

MISCELLANEOUS — These parameters are listed at the bottom of the OFFICE-DEPENDENT parameter table (Table 3.14-2). These are modes of operation and other office data that are not strictly timers.

3.14.1 Parameter Characteristics

Tables 3.14-1 and 3.14-2 provide the following information about each parameter:

- **Symbol:** The symbol that the CNI looks for in the network file to initialize the parameter.
- **Description:** A short description of the parameter function.
- **Bellcore ID:** The Bell Communications Research Identification, if available. This identification is for reference only. It is not used by the CNI.
- **Default:** The default value of the parameter.
- **Unit:** The units for the default value. When a new value is put in the network file, it must have the same units as the default value.

CAUTION: If a parameter is assigned a value outside of its appropriate range, an incorrect value is stored for that parameter and no error message is generated. The system may react inappropriately and unexpected, or unpredictable results may occur.

Table 3.14-1 Office Dependent User Changeable Parameters

SYMBOL IN NETWORK FILE	DEFAULT VALUE	BELLCORE ID	DESCRIPTION OF PARAMETER
Q704-T1	500 ms	T12	Trans. Delay Following Changeover
Q704-T2	700 ms	T11	Changeover Acknowledgement Timer
Q704-T3	500 ms	T15	Trans. Delay Following Changeback
Q704-T4	500 ms	T13	Changeback Ack. Timer (1st Attempt)
Q704-T5	500 ms	T14	Changeback Ack. Timer (Further Attempts)
Q704-T12	800 ms	T17	Uninhibit Ack. Timer
Q704-T13	800 ms	T18	Forced Uninhibit Ack. Timer
Q704-T14	2000 ms	T16	Inhibit Ack. Timer

Q704-T17	800 ms	T9	Timing to Restart of Initial Alignment
Q704-T19	180000 ms	T10	Time-Out for Attempting Link Activation
Q707-T1	1 sec	T19	Signaling Ring Test Ack. Timer
Q707-T1-Long	30 sec	T19	Long Ver. of Sig. Ring Test Ack. Timer
Q704-T6	5 (x100 ms)	T20	Controlled Routing Trans. Delay
Q704-T10	30 sec	T21	Sig.-Route-Set Test Mesg. Trans. Int.
Q704-T15	2 sec	T22	Transfer Controlled Update Timer
Q704-T16	1400 ms	T23	Sig.-Route-Set Congestion Test
The following parameters are special for setting the modes of operation and other office data that are not strictly timers.			
STP	0		Office is an STP (1= True, 0=False)
STD_PC	0		Office uses ANS [®] Standard Point Code (1=True, 0=False)
CS_NUM_CES	0		No. of Critical Events Allowed by SLMK per Time Period
CS_CE_TIME	0		Size of Time Period in Milliseconds For 5E5 Software Release. For 5E6 and Later Software Releases, the Size of the Time Period is in Seconds.

Table 3.14-2 Linkset Dependent User Changeable Parameters

SYMBOL IN NETWORK FILE	DEFAULT VALUE (AND UNITS)	BELLCORE ID	DESCRIPTION OF PARAMETER
Q703-T7	50 (x20 ms)	T1	Excessive Delay of Acknowledgement
Q703-T2	590 (x20 ms)	T2	Time for Out-of-Alignment Status
Q703-T3	590 (x20 ms)	T3	Time for Aligned Condition
Q703-T4a	115 (x20 ms)	T4	Normal Prove-In Period for 56 kb Links
Q703-T4b	30 (x20 ms)	T5	Emergency Prove-In Period for 56 kb Links
Q703-T1	650 (x20 ms)	T6	Timer for Aligned and Ready Condition
Q703-T5	4 (x20 ms)	T7	Busy Status Transmission Interval
Q703-T6	150 (x20 ms)	T8	Supervision of Busy State Timer
CC ABT1	820 bytes		Abatement Threshold Level 1
CC ABT2	7680 bytes		Abatement Threshold Level 2
CC ABT3	10855 bytes		Abatement Threshold Level 3
CC THS1	3072 bytes		Warning Threshold Level 1
CC THS2	8295 bytes		Warning Threshold Level 2
CC THS3	10956 bytes		Warning Threshold Level 3
CC DIS1	6042 bytes		Discard Threshold Level 1
CC DIS2	10855 bytes		Discard Threshold Level 2
CC DIS3	11571 bytes		Discard Threshold Level 3

3.14.2 How To Change A Parameter (5E8 And Earlier)

CAUTION: Modifications to the Network file for SS7 parameters should be made with caution and only under the direction or approval of ESAC or equivalent authority.

To change a protocol parameter, place the new value in the `database/cni/odata/network` file. The new value must have the same units as the default value. The network file contains one line for each parameter to be initialized, and as many lines as needed for comments. Comment lines begin with a pound sign (#) and are ignored. Each parameter line contains:

- A symbol.
- A value.
- For linkset-dependent parameters, the linkset number or the word ALL.

(Special international parameters have the words ALL_INTL_LKSET or ALL_DOM_LKSET).

The fields are separated by a tab or a space. This file is modified using the editor of the UNIX[®] RTR system. The general format of the network file is as follows:

```
#comments ended by a new line
#network indicator
<symbol> (tab or space) <value>
#point code standard indicator
<symbol> (tab or space) <value>
#Office type indicator
<symbol> (tab or space) <value>
#linkset-dependent data
<symbol> (tab or space) <value> (tab or space) <link set number or ALL>

(This field may have ALL_DOM_LKSET or ALL_INTL_LKSET, for those parameters that allow these options.)
<EOF>
```

- If the entry for a parameter is repeated two or more times in the network file, only the last entry has any effect. This is because parameters are read, processed, and stored in the order in which they appear. Therefore, the initialization caused by the first occurrence of a particular parameter is overwritten by the next occurrence.
- Once a change has been made, a CNI level 4 initialization is required to activate the new parameter values. During a level 4 initialization, CNI changes the parameter values in the central processor memory to the values specified in the network file. These values are sent to the nodes, as appropriate. These values remain in effect until the next initialization occurs. If an error occurs during the initializing of the parameters, the default values are used for all parameters and an error message is printed on the receive-only printer.

CAUTION: A CNI Level 4 initialization should be used very carefully since it can stop SS7 interswitch signaling entirely and can escalate to trigger an AM initialization.

NOTE: This feature does not provide any range checking of user specified parameters. Also, if an initialization occurs while the network file is being changed, unpredictable CNI operation may result. After the changes are completed, a level 4 initialization must be requested.

3.15 RECENT CHANGE OF PROTOCOL TIMERS AND PARAMETERS (RCPTP)

3.15.1 Description

The RCPTP feature provides the capability for the customers to change and verify the values of the Signaling System Number 7 (SS7) Message Transfer Part (MTP) and Signaling Connection and Control Part (SCCP) protocol timers and thresholds, two critical event parameters, and an *ANSI*[®] Point Code flag. These changes have immediate activation and do not require a system initialization or need for taking a link temporarily out of service.

3.15.2 Background

The SS7 and ITU-TS (formerly CCITT) protocols give recommended values and/or ranges for a number of timers and thresholds. Currently, these timers and thresholds can only be changed via the network file which has the following drawbacks:

- A Common Network Interface (CNI) initialization/system reboot is needed to activate any changes made to this file. If changes are needed more frequently because networks interconnect or because different default values are provided by different vendors' products at each end of the link, more unnecessary system down time results.
- No error checks are performed on the changes of the thresholds or timers. It is possible that some of the links may not come up after an initialization because of an invalid data.
- Making changes to the network file requires someone who knows the *UNIX*[®] system and the place where this file resides.

With RCPTP, these drawbacks are drastically reduced if not completely eliminated. In addition to the protocol timers and thresholds, the network file presently contains two critical event parameters, a signaling transfer point (STP) identifier and an *ANSI*[®] Standard Point Code flag. This feature makes the critical event parameters recent changeable, and removes the STP identifier since the 2STP has its own separate load lines. The *ANSI*[®] standard point code flag will be handled during retrofit, and a field tool will be updated to allow for any possible changes. The network file will then be empty and removed.

3.15.3 Availability

This feature is available with the 5E9(1) and later software releases.

3.15.4 Recent Change Views

Parameters which are badly tuned could degrade link performances and timer activation and operation.

The update of timers will cause links to be briefly taken out of service (these links are immediately restored).

CAUTION: Modifications for SS7 parameters should be made with caution and only under the direction or approval of ESAC or equivalent authority.

The parameters previously accessed via the network file have been placed on recent change views as shown in Table 3.15-1 :

Table 3.15-1 Recent Change View Numbers

TIMER OR PARAMETER	VIEW NUMBER
STD_PC CS_NUM_CES	15.1 Office Data View

CS CE TIME	
OFFICE DEPENDENT PARAMETERS	15.14 Protocol Office Timers 15.15 Protocol Linkset Timers
LINK SET DEPENDENT PARAMETERS	15.16 Protocol Linkset Thresholds 15.17 Protocol Link Parameters

Range checking is performed to insure that value is within the appropriate range for each parameter or timer. For LINK SET or LINK DEPENDENT parameters, a SCOPE field has been defined to allow the user to specify the granularity for the update. The values can be updated for ALL LINKS within the office, ALL LINKSETS, ONE LINK, or ONE LINKSET depending upon what timer is being updated.

3.16 MESSAGE TRANSFER PART ROUTING VERIFICATION TEST (MRVT)

3.16.1 MRVT Description

The purpose of the MRVT is to verify the consistency and accuracy of static message transfer part (MTP) routing data in SS7 networks. This helps to pinpoint routing problems. The MRVT procedure is part of the Operations and Maintenance Application Part (OMAP) which resides at the application layer of the SS7 protocol. The purpose of OMAP is to provide a set of SS7 protocol-defined procedures used for operation and maintenance of the network. The MRVT procedure resides under the OMAP functional area (similar to signaling traffic management residing under network management).

The MRVT detects any of the following problems in the SS7 network:

- Network blockage and congestion
- Loops and excessive length in routing
- Inconsistent routing data between adjacent signaling points
- Problems in data for forward and backward routing
- Local processing problems.

A simple view of MRVT could be stated as follows:

- Between any two signaling points [5ESS[®]-2000 switch, 4ESSTM switch, or signaling transfer point (STP)] in the network, a test can be initiated that verifies every possible route.
- The user enters the input message `EXC:MRVT` with appropriate parameters and the signaling point polls the CNI routing data for all possible paths to the terminating end.
- When the intermediate STP receives the `MRVT`, it also polls its CNI routing data for all possible paths to the terminating end.
- The STP propagates the message over all possible routes and sets timers for each message.
- As the `MRVT` messages reach the terminating end, the signaling point of the terminating CNI responds with a message routing verification acknowledgement (`MRVA`) message to the immediate sender of the `MRVT`.
- The terminating end signaling point sends out an `MRVA` for each `MRVT` message it receives.
- These `MRVA` messages are, in turn, sent back along the path to each specific signaling point in the route.

The OMAP uses the services of the Transaction Capabilities Application Part (TCAP). TCAP is defined as a communications protocol that provides rules and conventions for the exchange of application messages between network entities. The intent of TCAP is for noncircuit-related transactions.

The full requirements for network interconnect MRVT are still being negotiated, but a subset of network interconnect MRVT capabilities are provided on phase 1. This includes the ability of any signaling point within the local network to run the MRVT to verify MTP routing data at a nonlocal network signaling point. The MRVT proceeds up to the gateway STP without being transmitted into the nonlocal network, regardless of the TCAP compatibility of the nonlocal network.

Incoming MRVTs from nonlocal networks are screened by the STP based on office point code (OPC), destination

point code (DPC), and signaling connection control part (SCCP) subsystem only.

NOTE: No screening is done on the type of OMAP message.

If the screening function allows the message, the message is passed to OMAP. The OMAP process then determines if the TCAP protocol used in the MRVT message is compatible with the TCAP employed by the office. If it is compatible, the MRVT proceeds normally, including the transmission of all relevant MRVT messages across network boundaries. If not compatible, the MRVT message is simply dropped without further processing. Due to future network interconnect requirements, a TCAP interworking between ITU-TS (formerly CCITT) and ANS[®] is necessary, but is not provided on phase 1.

NOTE: The TCAP entity in the OMAP process performs the TCAP compatibility verification, not OMAP.

Sometimes an STP receives a signaling message to be routed for which the STP has no routing data (that is, unknown point code). For this type of message, the OMAP requires that the STP send an MRVR message (known as an unexpected MRVR) to the originator of the message. For phase 1, if the originator is in a nonlocal network, then no MRVR is sent. The received "unexpected" MRVR is processed only if TCAP compatibility exists.

The MRVT procedure is common to all signaling points within the SS7 network. Any office can be the initiator and any office can be the test destination (terminator).

The MRVT is initiated by using a maintenance person command. This can be on-site or through a support system. Currently, there are no requirements to automatically initiate the MRVT. All output messages are sent to the source of the initiation command and the maintenance output class.

The MRVT replaces the routing verification test (RVT).

The core of OMAP processing resides in the AM; that is, the CNI central processor. The MRVT operates on data stored in the CNI processor. Although MTP routing data resides in other types of CNI-maintained peripheral nodes (for example - DLN), the master copy is that in the AM. The STPs also derive their MTP routing data from the CNI copy in the AM; therefore, when performing MRVT functions at an STP, the CNI data is used.

The only other processor that is impacted is the SS7 node processor. Changes and additions must be made to distribute incoming OMAP operation, administration, and maintenance (OA&M) messages accordingly (that is, SCCP subsystem 4).

When the MRVT procedure is initiated by using a maintenance person command, the real-time reliable (RTR) UNIX[®] system program automatically accesses an MRVT process. This CNI-owned process examines the input command line to determine that it contains correct language. If successful, it notifies the OMAP process with an interprocess message switch (IMS) message. The MRVT procedure initiated by the maintenance person dies once it ensures that the OMAP process received the notification and correct parameters. The OMAP process contains all logical entities necessary to implement the MRVT, including TCAP. If the OMAP process determines that another MRVT initiation is possible, it generates the appropriate MRVT messages to the network. On the outgoing side, the SS7 node processor transmits the MRVT message without any additional processing other than the normal message handler transmit functions.

When incoming MRVT messages arrive from the network, SCCP in the SS7 node processor distributes the messages to the AM OMAP channel based on the subsystem number (all OMAP messages are assigned subsystem 4, according to protocol). On receipt of the corresponding MRVA messages (or on expiration of protocol timer T1), the OMAP process reports the results of the test. Again, the TCAP processing is handled by the OMAP process.

3.16.2 OMAP Process Characteristics

The operations and maintenance applications part (OMAP) resides in the AM memory and is UNIX[®] system

program level, permanent, swappable, and noncritical. This OMAP process does not have scheduled work on an ongoing basis, but rather is invoked when some maintenance-type procedure is initiated. The output of MRVT is expected to be small; hence, the load on the spooler output process (SOP) and controller SOP (CSOP) is minimal. So, the OMAP process priority is set at 176, just below the maintenance person processes, but above the SOP and CSOP processes.

The process is permanent because at any time, an "unexpected" MRVR message can be received, not just when an office initiates an MRVT. For availability reasons, the OMAP process is noncritical, since this function is not critical to the basic fundamental processing of an office. The OMAP process attaches to the CNI shared library (CNISHRLIB).

The OMAP process opens an interprocess message switch channel that is exclusively for CNI OMAP transactions. This channel is opened on process creation and is kept open indefinitely. The OMAP process performs all TCAP processing that pertains to the MRVT. This TCAP processing is specific to CNI and the MRVT. The CNI does NOT provide a TCAP entity that can be used by the applications for other features. The network control point (NCP), 4ESSTM switch, 5ESS[®]-2000 switch, and 1A ESSTM switches already have their own TCAP entities.

The OMAP process allocates a TCAP indicator data item used to determine which version of TCAP the OMAP entity for that particular office is employing. This indicator is set by the OMAP process at initialization.

There is a need to attach to the protected application segment (PAS) to gain access to the MTP routing data by using primitives; access mode is read-only. Since routing data is the only data in PAS that needs to be accessed, the PAS access mode is read-only.

3.16.3 MRVT Process Characteristics

The MRVT process also resides in the CNI AM and is used to handle the maintenance person command that initiates the MRVT. It is a noncritical, transient (nonpermanent), UNIX[®] system program level process. The priority is set to 184, which is the same for other maintenance person processes. This process simply checks the input command for proper language and notifies the OMAP process of the MRVT request by using interprocess message switch.

After the input MRVT parameters have passed validation, the MRVT IMS channel is opened by the MRVT process and used to send the message to the OMAP process. Once it has been assured that the IMS message has been written, the channel is closed and the MRVT process dies. The channel can now be used by another MRVT maintenance person process. Contention for the one MRVT IMS channel is rare since that simultaneous initiation of MRVTs is improbable. Should this happen, however, the MRVT maintenance person process that was "closed-out" again attempts to open the MRVT maintenance person channel; if the retries continue to fail for a reasonable number of attempts, the closed-out MRVT initiator is asked to reenter the initiation request.

3.16.4 Administration Of Delay Parameter D

Parameter D is used to calculate the value of timer T1. It is required that parameter D be recent changeable. The CNI is solely responsible for recent changing parameter D by using a maintenance person command, without a need for an interface to the applications.

3.16.5 Impact Of Initializations

The basic strategy on initializations is to recover gracefully without concern for an in-progress MRVT. Moreover, initialization "recovery" would require using a protected application segment (PAS), which is a premium resource. Therefore, the MRVT global data is not to be kept in PAS, but internal to the OMAP process.

On initialization level 1 (IMS channels are closed and reopened), the current MRVT status is not changed, but it is likely that MRVA/MRVR messages may be lost. This could result in misleading output messages and an incorrect diagnosis.

On initialization level 2 (all CNI processes are recreated, and shared libraries are read in), it may be possible to receive an MRVA or MRVR message after the OMAP process is recreated. Because the OMAP process has no record of a previous transaction, this could also generate misleading output messages.

On initialization levels 3 and 4, it is extremely unlikely (not even possible given our current initialization times) to receive a "straggler" MRVA or MRVR message.

It is suggested that the maintenance persons initiating the MRVT command be aware of any initialization levels during the MRVT so they may rerun the test. Do not be misled by MRVT output messages after the initialization, but before a new MRVT initiation. It is not good practice to generate misleading messages, but this is a rare occurrence.

3.16.6 Reliability

Because the MRVT has a distributed architecture with some form of interprocess/interprocessor communication, reliability cannot be guaranteed. That is, because of IMS limitations, there cannot be 100 percent assurance of message delivery among processes and processors. However, the probability of lost messages is small. Also, since MRVT is not deemed critical to the functioning of the office, reliability is not an issue.

3.16.7 Availability

Because the MRVT consists only of noncritical processes, availability is not affected. Initialization times do not increase (initialization time is measured from the onset to the final CRITICAL process being created). If the OMAP process has a malfunction and dies, it is recreated automatically by CNIINIT without any impact on the system. The MRVT processes only read (and do not write) the shared MTP routing data in PAS.

3.16.8 Input Message Formats

This input message changes or displays the MRVT delay (D) parameter which is used in the calculation of the T1 timer. The 235-600-700 , *Input Message Manual* contains the MRVT input message formats and an explanation of the message details.

If a request is made to change the delay parameter and it is within range, the requested value is written onto disk and the delay parameter is updated to the new value.

The internal design of the MRVT recent change process input/output references is as follows:

- Input messages:

- CHG:MRVT
 - EXC:MRVT-PC

- Output messages:

- CHG:MRVT
 - EXC:MRVT-PC-STPS
 - REPT:MRVR

The requested test is run and the report is written to the maintenance class and/or the standard output.

3.16.9 Output Message Formats

The 235-600-750, *Output Message Manual* contains the formats of the CH:MRVT and the EXC:MRVT output messages and an explanation of the messages and definitions of the variable field entries.

The OMAP protocol specifications are as follows:

- Input Messages:

- CHG:MRVT

- EXC:MRVT

- Output Messages:

- CHG:MRVT

- REPT:MRVR

3.16.10 Report Of Message Transfer Part Route Verification Result Message

Following is the message transfer part (MTP) route verification test result message report description. The 235-600-700, *Input Message Manual* and 235-600-750, *Output Message Manual* contain the format and description of the MRVR report message and definitions of the variable field entries.

When this report is received, collect the data from the receive-only printer and request technical assistance. Note that this causes a minor alarm.

The input/output manual references are as follows:

- Input Messages:

- CHG:MRVT

- EXC:MRVT-PC

- Output Messages:

- CHG:MRVT

- EXC:MRVT-PC-STPS

3.17 SIGNALING CONNECTION CONTROL PART ROUTING VERIFICATION TEST (SRVT)

3.17.1 Description

The signaling connection control part (SCCP) is a component part of SS7 protocol. It provides additional functions to those made available by the message transfer part (MTP) to offer network services used for transferring signaling information between switches, data bases and other signaling points. Whereas the MTP provides basic message routing capabilities on a link-by-link basis, the SCCP provides specialized routing capabilities which form the basis for design of data base services in the SS7 network. An important SCCP function involves global title translation capability provided by the STPs and switches in the SS7 network.

The global title consists of information contained in the signaling message that can be used by the SCCP to perform a translation to determine the destination of the message. The translation gives the identity of the destination point code and the subsystem number of the application residing at that destination. When the message reaches its intended destination signaling point (SP), the destination SP sends a response message which may provide instructions and/or the destination routing address that the switch needs to complete the call. The global title translation (GTT) serves to provide a flexible way to introduce new services in the network. The SRVT is an OMAP test procedure dedicated to verifying the SCCP capability pertaining to GTT and other conditions (for example, loop, excessive length) necessary to verify the success of the SCCP query/response communication in the SS7 network.

This routing verification provides the means for testing the GTT data for accuracy, completeness, and consistency. In this process, the procedure also detects errors, such as the following:

- Loops and excessive lengths in the SCCP routing.
- Unknown destinations as identified by Global Titles.

The SRVT uses the following three OMAP test messages, specified by the application service element (ASE):

- SCCP Routing Verification Test (SRVT) Message.
- SCCP Routing Verification Acknowledgement (SRVA) Message.
- SCCP Routing Verification Result (SRVR) Message.

The SRVT message serves the following three different roles:

- The Request form of the message is sent by the test initiating SP to request a global title translation. The destination of this message is a translation signaling point (TSP). If there is more than one translating point in succession, the Request form of the message is also sent from an intermediate translation signaling point (ITSP) to a final translation signaling point (FTSP).
- The Verify form of the message is sent by the FTSP to the destination signaling point.
- The Compare form of the message is sent by a translation signaling point (TSP) to its mate TSP to compare results of duplex translation at the mated pair of STPs.

The SRVA is a message sent in the backward direction on a hop-by-hop basis, (such as, the recipient of an SRVT message sends SRVA to the sender of the SRVT message, informing the sender of the success of the test, or, in the case of failure, the cause of the failure).

The SRVR is a message sent in the backward direction by the destination SP or an enroute SP detecting a failure

to the SP initiating the test. This message contains the identity of the TSPs along the route taken by the SRVT message from the initiating SP to the tested destination or another SP identifying a failure, referred to as route trace information. Additionally, the message contains the results of the test, success, or failure. In case of failure, it identifies the cause.

Thus, the accuracy and completeness of the global title translation data are verified by forward and backward messages. The consistency of data at mated TSPs is verified by `Compare` messages. It should be remembered that the SRVT verifies routes at the SCCP level only. The MTP Routing Verification Test (MRVT) is necessary to verify routing at the MTP level of the network.

If the SRVT capability is not simultaneously present in all network elements (for example, 4ESSTM switch, STP, 5ESS[®]-2000 switch, and NCP), a recipient SP, not having SRVT capability, can discard the message without harm to the network. However, the test initiator may receive confusing results with the possibility that time is wasted chasing problems which may be nonexistent.

3.17.2 SRVT Characteristics

C Link Failure: If an STP finds its mate inaccessible for the routing of a compare message, the test continues. The STP times out and then sends SRVR and SRVA messages. The error reported is `Timer Expired`.

Response to SRVT from an SP with no SRVT Capability: No significant response to the initiator, the initiating SP times out and provides the results to the initiator.

SRVT Messages across Network Boundaries: Currently, SRVT is valid only in the intranetwork mode. If an STP in the NSD network receives an SRVT message from an SP in a nonlocal network, it discards this message. An STP acting as a TSP is required to detect an SRVT message destined to cross the network boundary. The STP reports this as a `Route Inaccessibility` error.

Characteristic of Data Checked: The SRVT checks the master copy of administered (not dynamic) translation data.

Routing of SRVR Messages: The protocol states that the SRVR message is routed to the initiator using the initiator's PC if the MTP backward routing required indicator is set and the initiator's PC is recognized. If the MTP backward routing required indicator is not set or the MTP backward routing required indicator is set and the initiator's PC is not recognized, the reported error is `unknown initiator`.

Reporting of Test Results: Each error is identified in the SRVR and SRVA message. The SRVA message is able to report more than one error. The SRVR reports only one error. In the case of failure or partial success, the SRVA always contains the information regarding SRVR sent or not sent. The SRVR contains the PC of the SP where the error was detected. It may contain a trace of the TSPs. The printout report lists separately each SRVA and SRVR message received at the initiating SP. If the initiating SP is a duplex TSP, and receives an SRVA Compare message from its mate, this message is included in the SRVA messages listed. The declaration of `Success` takes place at the tested destination if the procedure is successful, no errors have been detected, and no failures encountered in sending back the SRVR and SRVA messages from the destination.

NOTE: Even if the tested destination has declared `Success` in the SRVR to the Initiator, the Initiator also gets an SRVR and an SRVA from a duplexed TSP indicating FAILURE, if the results of the `Compare` message show a mismatch in the global title translation data between the mated pair. This is because the duplexed TSP forwards the SRVT message to the tested destination before receiving and analyzing the results contained in the SRVA from its mate.

Error in SRVT Initiation: This error is detected at the initiator SP. The error pertains to the validity of the data in the SRVT command.

Loop: An SCCP routing loop is detected when an STP acting as a TSP examines the list of crossed TSPs in the

SRVT message and finds that the PC of the next TSP or that of its mate is already on the list.

Excessive Length Route: This condition is detected by an STP acting as a TSP when, before forwarding the SRVT to the next TSP or to the destination SP, it examines the list of crossed TSPs and finds that the number of crossed TSPs equals or exceeds the threshold value.

No Translation for Global Title: This error is detected when there is no PC corresponding to this GT at the ITSP, or no PPC+SSN or SPC+SSN corresponding to this GT at the FTSP.

Inaccessible Signaling Point: This error is also referred to as `route inaccessible`. It is detected at the initiator SP or at a TSP. It is never reported from the destination SP. One or more of the following conditions applies:

- Congestion: The route selected is congested and message priority does not permit its transmittal.
- Blockage: All routes are blocked, [for example, as a result of link set failure, or the destination SP has entered signaling point isolation (SPI)].
- Crossing Network Boundaries: Not allowed, restriction is the responsibility of the STP, not the switch.
- Not SS7 Equipped: Treated as `route inaccessible` for purposes of reporting by using SRVA or SRVR.
- Subsystem Prohibited: Treated as `route inaccessible` if the SRVT is destined for a prohibited subsystem.
- Received Unit Data Service Message: Treated as `route inaccessible` when a unit data service message is received in response to an SRVT message sent.

Test Cannot Be Run Due To Local Conditions : This error results if a test cannot be initiated at an initiating SP or continued at a TSP. The following lists such local conditions:

- Processor overload.
- The test pertains to a GT already under test.
- Threshold for maximum number of initiations at an SP has been exceeded.

Unknown Initiating Signaling Point: This error is detected at the tested destination or at an STP acting as a TSP. At a TSP receiving an SRVT, where the MTP backward routing indicator was not set, or if the MTP backward routing indicator was set but the initiator point code is not recognized, then the SRVR cannot be sent. The error Unknown Initiating Signaling Point is identified in the SRVA message returned by the SP.

Timer Expired: The error condition `timer expired` (also referred to as Time-out waiting for SRVA) is detected at the initiating SP or a TSP. It does not apply to the tested destination. The SRVR message also contains the point code of the SP which did NOT send the SRVA.

Message Arrived at the Wrong Signaling Point : If any SP which is not a duplexed TSP receives a `Compare` form of SRVT, or a duplexed TSP receives a `Compare` form of SRVT from a TSP which is not its mate, it reports this error to the Initiating SP. If a `Request` form of SRVT arrives at an SP which is not a TSP, it also reports this error. If a `Verify` form of SRVT arrives at a TSP or any SP which is not the tested destination, it reports this error.

Incorrect Translation for Primary Destination : This error is detected by the mate of a duplexed FTSP and indicates that the translation results pertaining to PPC+SSN at the mate does not match with the results at this FTSP. The error is identified in the SRVA. The SRVR identifies the mate performing the comparison and identifies the error.

Incorrect Translation for Secondary Destination : This error is detected by the mate of a duplexed FTSP. It is similar in all respects to Primary Destination error except that it indicates that the translation results pertaining to SPC+SSN (rather than the PPC+SSN) at the mate does not match with the results at this FTSP.

Incorrect Translation for the Intermediate TSP: The error is detected by the mate of a duplexed ITSP and indicates that the translation results pertaining to PPC, SPC, or both, does not match with results at the ITSP. The SRVR identifies the mate performing the comparison and identifies the error.

Not Primary Destination: This error is detected at the primary of a mated pair of NCPs/SCPs when the NCP/SCP determines that it does not serve the GT as the primary destination. The error is also reported by a non-mated NCP/SCP, or a switch, when it determines that it does not serve the Global Title contained in the SRVT.

Not Secondary Destination: This error is detected at the secondary of a mated pair of NCPs/SCPs when the NCP/SCP determines that it does not serve the GT as the secondary destination. The error is also reported by a non-mated NCP/SCP, or a switch, when it determines that it does not serve the Global Title contained in the SRVT.

Primary Destination Not Recognized: The error is detected at the secondary of a pair of mated NCPs/SCPs when the NCP/SCP determines that it does not recognize the PPC+SSN as the primary destination for the GT contained in the SRVT. (It DOES recognize the SPC+SSN as the secondary destination of the GT which it serves.)

Secondary Destination Not Recognized: The error is detected at the primary of a pair of mated NCPs/SCPs when the NCP/SCP determines that it does not recognize the SPC+SSN as the secondary destination for the GT contained in the SRVT. (It DOES recognize the PPC+SSN as the primary destination of the GT which it serves.)

Unrecognized Point Code from Translation : This error is detected at a TSP when it cannot route on the point code realized from the global title translation.

3.17.3 SRVT Limitations

Test Initiator: An SP is allowed to initiate no more than five simultaneous SRVTs to different GT destinations.

Translation Signaling Point: The STP is allowed to process no more than 25 concurrent SRVT tests. This includes five tests allowed as an initiating SP.

Destination SP: There shall be no limit on the number of concurrent SRVT tests allowed to terminate at a destination SP.

3.17.4 Input Message Formats

3.17.4.1 CHG:SRVT

This message requests that the SCCP Routing Verification Test (SRVT) delay parameter, which is used in the calculation of the T2 timer, be changed or displayed. The expiration of the T2 timer signifies the end of the waiting period for the reception and processing of all expected SCCP Routing Verification Acknowledgement (SRVA) messages.

If a request is made to change the delay parameter, and the requested value is within range, it is written onto disk and the delay parameter is updated to the new value. This new value becomes the new "default," that will be read in on initializations. The initial default is 12.

For more information, refer to input messages EXC:SRVT, OP:TPC, and output messages CHG:SRVT, EXC:SRVT, OP:TPC in the 235-600-700, *Input Message Manual* and 235-600-750, *Output Message Manual*.

3.17.4.2 EXC:SRVT

This message requests that the SCCP Routing Verification Test (SRVT) be initiated.

For more information, refer to input messages CHG:SRVT, OP:TPC, and output messages CHG:SRVT, EXC:SRVT, OP:TPC.

3.17.4.3 OP:TPC

This message requests Translation Point Codes (TPCs) for the specified Translation Type (TT) be displayed.

For more information, refer to input messages CHG:SRVT, EXC:SRVT, and output messages CHG:SRVT, EXC:SRVT, OP:TPC.

3.17.5 Output Messages

3.17.5.1 CHG:SRVT

The formats for this message are as follows:

- (1) CHG:SRVT DELAY PARAMETER SET TO a SECONDS
- (2) CHG:SRVT REQUESTED DELAY PARAMETER, a, OUT OF RANGE DELAY PARAMETER RANGE IS 8 - 16 SECONDS INCLUSIVE

Format 1 is printed when a valid CHG:SRVT command is entered, with or without the optional delay parameter specified.

Format 2 is printed when the range of the input is outside the permissible limits (8 - 16 seconds).

The variable field definition a is the requested or current value of the SCCP routing verification test (SRVT) delay parameter, in seconds.

For Format 1, there is no action to be taken because it is for information only.

For more information, refer to input messages CHG:SRVT, EXC:SRVT, OP:TPC, and output messages EXC:SRVT, OP:TPC.

3.17.5.2 EXC:SRVT

If no translation point code (TPC) is specified in the initiation command and the initiating signaling point (SP) does not know how to obtain the global title translation (GTT) for the specified global title (GT), the SP responds with UNABLE TO DERIVE TPC and (in case of error in data entered in the initiation command) followed by an appropriate indication identifying parameter(s) in the initiation command found to be in error by the SP. Otherwise, one of the formats is possible. These formats are presented for two cases: When one SCCP routing verification test (SRVT) request or verify message was sent, Formats 1-3, and when two messages were sent for a single SRVT initiation request, Formats 4-6. Formats 1 and 4 are used when the SRVT was successful and the SRVT user did not request a trace. Formats 2 and 5 are used when the SRVT was successful and the user requested a trace. Formats 3 and 6 are used when either partial success or failure occurred. For more information, see input messages CHG:SRVT, EXC:SRVT, OP:TPC, and output messages CHG:SRVT, OP:TPC.

3.17.5.3 OP:TPC

Format 1 of the OP:TPC message is used when a specific translation type is entered. Format 2 is used when the word ALL appears as the translation type.

NOTE: When the `ALL` option is used, only equipped translation types are printed, the other translation types will use the default TPCs.

The variable field definitions are as follows:

- The translation type.
- A translation point code (in decimal notation), or `UNABLE TO DERIVE TPC`.
- An optional translation point code (in decimal notation), or not displayed at all.

For more information, refer input messages `CHG:SRVT`, `EXC:SRVT`, `OP:TPC`, and output messages `CHG:SRVT`, `EXC:SRVT`.

3.18 DIRECT LINK NODE 30 (DLN30)

3.18.1 Description

The Direct Link Node 30 (DLN30) feature provides support for higher SS7 capacity, which includes ISUP and TCAP applications, on the switch. This capacity increase is accomplished by replacing Small Scale Integration (SSI) nodes on the CNI ring.

3.18.2 Availability

The DLN30 secured feature is available beginning with software release 5E9(2).

3.18.3 Feature Application

3.18.4 Feature User

This feature has been designed for use by switch maintenance personnel.

3.18.5 Feature Operation

This feature includes the following hardware upgrades to the CNI ring:

- The DLN attached processor (AP) is replaced with newer technology, the *Motorola*® 68030 or AP-30, which increases the DLN memory from the existing 2 MB to 16 MB.
- The DLN's SSI-based ring interface is replaced with an Integrated Ring Node 2 (IRN2). The IRN2 upgrade must accompany the AP-30 upgrade, as the IRN2 is necessary for the DLN to deliver the required performance.
- Eight-node or five-node IRN2 shelves replace the current shelves. The eight-node shelf is optional and is deployed when additional link node capacity is needed. The new all-IRN2 shelf arrangement is shown in Figure 3.18-1.
- The DLN30 can handle up to 100,000 trunks. A DLN is required for capacities greater than 80,000 calls per hour.

Shelf 5

Group 34	P W R		LN 34 1	LN 34 2	LN 34 3	LN 34 4	LN 34 5	LN 34 6	LN 34 7	LN 34 8	I F B	P W R

Shelf 4

Group 33	P W R		LN 33 1	LN 33 2	LN 33 3	LN 33 4	LN 33 5	LN 33 6	LN 33 7	LN 33 8		P W R

Shelf 3

Group 32	P W R	I F B	RPCN32-0			LN 32 1	DLN32-2			LN 32 3	LN 32 4		P W R

Shelf 2

Group 02	4 1 0 A A		U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	T N 1 8 0 3	4 1 0 A A

Shelf 1

Group 01	4 1 0 A A		U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6	4 1 0 A A

Shelf 0

Group 00	4 1 0 A A	T N 1 8 0 3	U N 3 0 4 B		T N 9 1 4	T N 6 9 B	U N 3 0 4 B		T N 9 1 6	U N 3 0 4 B		A P 1 6 3 0	T N 9 1 4	T N 6 9 B	U N 3 0 4 B	T N 9 1 6	U N 3 0 4 B	T N 9 1 6		4 1 0 A A

Figure 3.18-1 IRN2 CNI Ring

These hardware upgrades:

- increase the CCS7 message handling capacity of the CNI ring,
- increase the number of CCS7 link terminations by using the IRN2 technology and a new IRN2 shelf arrangement to nineteen link pairs, and
- increase DLN memory, which will result in an increase in trunk translation data allocation in the DLN.

As a result, there is a significant increase in the number of usable CCS7 trunks on the switch. Currently, the number of CCS7 trunk terminations on the switch are limited by available DLN memory for trunk data. However, this feature does not make any enhancements to the link capacity on the switch.

3.18.6 Compatibilities

This feature only supports CCS7 IRN2 nonencrypted LNs (TN916) that have the PRO feature.

3.18.7 Cross References

The 5ESS®-2000 switch CCS7 Capacity Improvement - DLN30 Feature Candidate number is 99-5E-1136.

3.19 MTP NODE RESTART FEATURE

3.19.1 Feature Description

The MTP Restart procedure, feature 99-CP-2314, enables the Message Transfer Part (MTP), at a signaling transfer point (STP) that has just become available, to bring sufficient signaling links into the available state to handle the expected traffic and to stabilize its routing before user traffic is restarted to the STP.

MTP Restart procedures may also be performed at signaling points adjacent to the signaling point which is restarting. These procedures are not needed at a restarting signaling end point (SEP), but are provided for a SEP adjacent to a restarting signaling point.

This procedure uses two messages:

- Traffic Restart Waiting (TRW) message — Notifies the receiving signaling point that user signaling traffic (that is, traffic from the users of the MTP, such as ISUP) should not be sent until a traffic restart allowed (TRA) message is received from the originating signaling point.
- Traffic Restart Allowed (TRA) message — Notifies the receiving signaling point that user signaling traffic may be resumed to the originator of the message.

This is a secured feature (SFID=177) and a right-to-use (RTU) fee must be paid to Lucent Technologies before enabling information is provided.

3.19.2 Cross References

This feature is associated with the following Bellcore requirements:

TR-NWT-00606, "Common Channel Signaling," Section 6.5, Bellcore, Issue 2, October 1992

Section 9 of T1.111.4 provides *ANSI*[®] requirements for MTP Restart procedures. *ANSI*[®] requirements can be found in

TR-NWT-000246, "Bell Communications Research Specification of Signaling System Number 7," Bellcore, Issue 2, June 1991, plus Revisions.

3.19.3 Background

The Signaling Network Systems (SNS) Committee of the Federal Communications Committee (FCC) Network Reliability Council, T1S1.3 provides CCS network architecture evaluations and SS7 protocol enhancements. In the interest of facilitating uniform industry deployment, a SNS subgroup prioritized enhancements into two levels. The MTP Restart feature is one of the features in the high priority level.

3.19.4 Availability

This feature is distributed in the 5E11 software release.

3.19.5 Feature Environment

This feature is provided per switch.

3.19.6 Feature Operation

3.19.6.1 Description of Operation

Signaling route status information may be lost or network failures may occur during the time a STP is unavailable. This would cause a newly available STP to have inaccurate routing information or be unaware of the status of a number of signaling routes.

The primary reason for initiating a MTP Restart procedure, at a newly available STP, is that every STP has a mate that can process all of the user signaling traffic and fewer messages would be lost during restart if the available mate continues to process traffic until the restarting STP reaches stability.

Signaling points adjacent to the unavailable STP must recognize the unavailable state of the STP if the restart procedures are to be effective. A signaling point recognizes that another signaling point is unavailable when it can't be reached via any route. The unavailable STP must attempt to ensure that adjacent signaling points recognize its unavailable state by continuing to remain unavailable for a predetermined time period. This allows adjacent signaling points time to receive transfer prohibited messages pertaining to the unavailable STP, from the unavailable STP's mate, as well as time to recognize that the direct link set to that STP is unavailable.

From the perspective of a signaling end point (SEP), adjacent to a restarting STP, when the first link of a link set, to a previously inaccessible STP, becomes available and the SEP is ready to receive signaling traffic the SEP sends a traffic restart allowed (TRA) message to the restarting STP. The SEP will then wait for a TRA message from the restarting STP before sending signaling traffic.

3.19.6.2 Timers

There are three new per-office (level 3) timers, (T25, T28, and T29) which are set using recent change procedures. See Table 3.19-1 for a list of timers and default values.

Table 3.19-1 Signaling End Point (SEP) Timers

Timer	Description	Default Value	Range
T25	Timer at SEP adjacent to restarting STP, waiting for traffic restart allowed (TRA) message	32 sec	0-60 sec
T28	Timer at SEP adjacent to restarting STP, waiting for traffic restart waiting (TRW) message	5 sec	0-60 sec
T29	Timer started when TRA sent in response to unexpected TRW/TRA or no TRA received when traffic is restarted	62 sec	30-90 sec

3.19.7 User Operation

Switch personnel will use recent change procedures to unlock the security, enable the feature and set the appropriate timers.

3.19.8 Engineering

3.19.8.1 Hardware Resources

No hardware considerations are associated with this feature.

3.19.8.2 Software Resources

No software considerations are associated with this feature.

3.19.8.3 Transition Considerations

In the transitional period, where not all signaling points in the CCS networks have the MTP Restart procedures implemented, restarting signaling points may receive user signaling traffic during restart, and this could hinder the restart procedures.

3.19.9 Interactions and Limitations

No interactions have been identified.

3.19.10 Incompatibilities

There are no incompatibilities associated with this feature.

3.19.11 Dependencies

No dependencies have been identified.

3.19.12 Isolation Constraints

Not applicable.

3.19.13 Feature Implementation

3.19.13.1 Office Data Administration (ODA) Provisioning

There is no ODA provisioning associated with this feature.

3.19.13.2 Recent Change Provisioning

The service provider must unlock this secured feature and activate the feature using recent change procedures.

Unlock the security lock for the feature by populating Recent Change view 8.22, *Secured Feature Upgrade*:

FIELD	VALUES
FEATURE ID	177
MODULE	(OFC or SM 1-192)
PASSWD	(Obtain from Lucent Technologies SFID Administrator)
ACTIVE	Y

"Y" - Turns on (unlocks) the feature

"N" - Turns off (locks) the feature

Activate the feature using Recent Change view 8.15, *CCS Office Parameters*:

FIELD	VALUES
MTP NODE RESTART	Y (Default=N)

"Y" - Turns on (enables) the feature

"N" - Turns off (disables) the feature

Set the timer values using Recent Change view 15.14, *Protocol Office Timers*:

FIELD	VALUES
T25	32 (Range=0-60 secs.)
T28	5 (Range=0-60 secs.)
T29	62 (Range=30-90 secs.)

* See 235-118-2xx, *Recent Change Reference* for detailed information on allowed values.

3.19.13.3 Customer Premises Equipment (CPE)

No CPE is required for this feature.

3.19.14 Maintenance Considerations

Maintenance personnel can initiate and stop the MTP Restart procedure manually from the remote maintenance OS and manually retrieve the measurements. This feature adds three new messages to report STP operations.

- REPT:MTP RST - Commencement of MTP restart procedures
- REPT:STATUS RSTRT - Progress of MTP restart procedures (every 30 seconds)
- RCVRY:MTP RSTRT - Completion of MTP restart procedures

For a detailed description of messages, format and parameters, refer to 235-600-700, *Input Messages Manual* and 235-600-750, *Output Messages Manual*.

3.19.15 Administration

3.19.15.1 Measurements

This feature does not add any new measurements for a SEP.

3.19.15.2 Billing

This feature does not impact billing.

4. SIGNALING LINKS

This section provides information for setting up the signaling links when establishing or growing the common network interface (CNI) ring. The setup procedures include adding and rearranging analog and digital signaling links.

4.1 DESCRIPTION

4.1.1 Digital Signaling Links

Digital signaling links operate at 56 kb/s. The part of the signaling link between the ring node and the transmission facility is made up of a TF9 digital service adapter (DSA) circuit pack, and a digital service unit (DSU) used with a combined DSU/channel service unit (CSU), or equivalent. Figure 4-1 shows the physical makeup of a digital signaling unit. The digital A-links, unlike the analog A-links, are not dual links (there are no standby links).

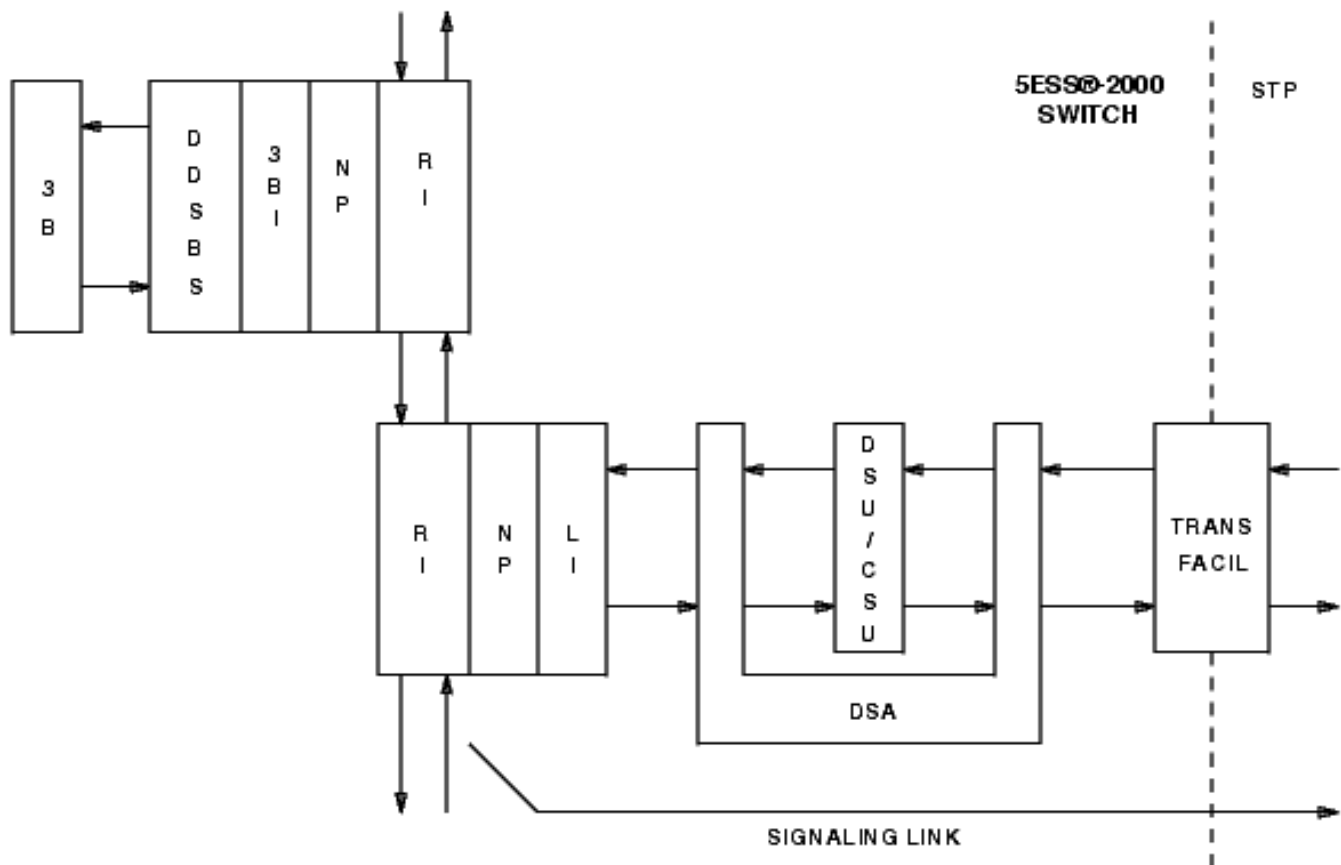


Figure 4-1 Digital Signaling Link Block Diagram

The length of the signaling link determines whether a CSU and/or transmission facilities are needed. When transmission facilities are not used, internal timing must be provided on the DSUs.

Figure 4-2 is a block diagram showing the signaling link used with the switch.

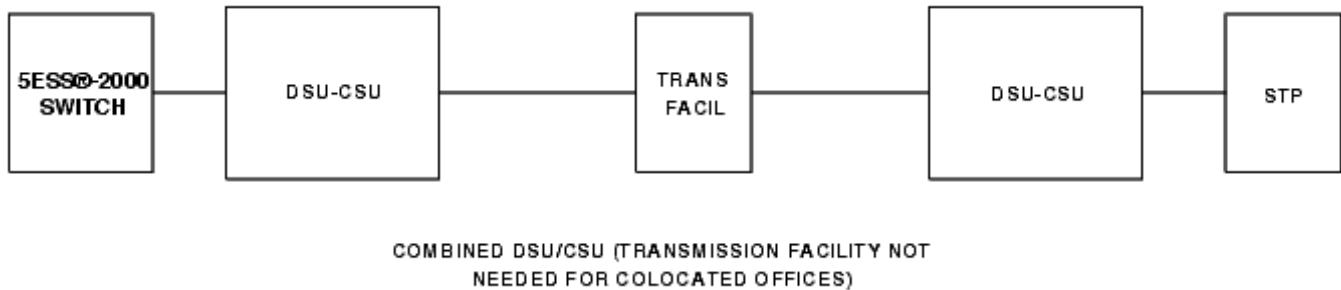


Figure 4-2 Digital Signaling Links

4.2 IMPLEMENTATION

4.2.1 Facility Access Assignments

The paired signaling links and links from the same location are separated according to power diversity within the cabinets. Following are some general guidelines for assigning signaling links (A-links) within the analog facility access frame and the digital facility access cabinet:

- Since these links are provided with dual facilities (except for 56 kb/s applications), assignments are not restricted.
- If there are more than one layer from the same location, they should be assigned to different cabinets and different power buses, where possible.

4.2.2 Signaling Link Diversity Requirements

Signaling link diversity is required to assure signaling network availability objectives. Two-way diversity is necessary for A-links. The linkset between the 5ESS®-2000 switch to one 2ASTP should be on diverse facilities from the linkset between the switch and the mate 2ASTP. This would prevent an office from being isolated from the mated 2ASTPs because of a transmission facility failure.

4.2.3 Signaling Link States

There are three major states in which a signaling link can exist as follows:

- **UNEQUIPPED:** In this state, the link node (LN) has no link configuration data in main memory or on the disk. When link data is added, the LN is automatically put in the **UNAVAILABLE - Grow** state. The Recent Change View 15.2 can be used for removing the link data, and also Field 13. When the line data is removed, the link status changes to the **UNEQUIPPED** state. During a CNI level 4 boot, all links that do not have any link data are automatically put in the **UNEQUIPPED** state.
- **UNAVAILABLE:** The signaling link must be in this state for the user to change the link data. While in this state, if band translation has been made, switching offices can perform preservice common channel signaling (CCS) trunk testing. Signaling link diagnostics can also be run.

Two minor link states are associated with this major state.

- **Grow:** While in the grow state, no link usage information is provided to the user (that is, loss of sync and automatic changeover). Although signaling links may have passed their installation test, if they are not ready for preservice testing, they should be left in the **UNAVAILABLE - Grow** state.
- **Test:** When the signaling link is ready for preservice testing, it is moved to the **UNAVAILABLE - Test**

state. While in this state, the signaling link provides the user with link usage information but does not interact with the network or provide alarms. This allows only its own sync signals to be acknowledged.

- **AVAILABLE:** In the available state, there are three minor signaling link states as follows:
 - **Out Of Service (OOS):** When the signaling link is ready to be made available for service, it is moved from the **UNAVAILABLE** state to the **AVAILABLE - OOS** state via Recent Change View 15.2 and diagnostics are automatically run. The man-machine language (MML) or program documentation standard (PDS) may be used to move the link from one state to another. When an error condition occurs on a signaling link that is in service, the system automatically moves the signaling link to the **AVAILABLE - OOS** state and attempts to restore the link. If the attempts to restore the signaling link fail, manual intervention is required.
 - **In Service (IS):** If the signaling link passes all the diagnostics, it is moved to the **AVAILABLE - IS** state. The signaling link is now ready for service.
 - **Manual Out Of Service (MOOS):** If it is necessary to work on a signaling link, the link must be removed from service. Depending on the traffic load and the availability of the mate link, the system will allow or disallow the signaling link to be moved to the **AVAILABLE - MOOS** state.

Table 4-1 shows the transactions that can be made from one signaling link state to another. The signaling link is moved from one state to another by accessing the data base forms using recent change (RC). An asterisk in a column in the **AVL-OOS** row, indicates that the signaling link is always moved first to the **AVL-OOS** state when changing from any state to the **AVAILABLE - IS** state.

Table 4-1 Signaling Link State Transitions

FROM → TO	UNEQP ^a	UNAVL GROW	UNAVL TEST	AVL MOOS	AVL OOS	AVL IS
UNEQP	-	A	A	NA	NA	NA
UNAVL GROW	A	-	A	NA	NA	NA
UNAVL TEST	NA	A	-	A	NA	NA
AVL MOOS	NA	NA	NA	-	A	A
AVL OOS	NA	T	T	T	-	A
AVL IS	NA	A	A	A	A	-
Notes: a. A = Allowed NA = Not Allowed T = Transient state used when changing states.						

4.3 SIGNALING LINK MANAGEMENT

Signaling link management is the function of establishing, maintaining, and restoring signaling links after a link failure.

One function of signaling link management is to keep the signaling traffic balanced among signaling links between points in the network. This is accomplished by engineering the CCS network so that there are several signaling links over which signaling messages can travel between an originating and destination point in the network. Groups of (from 2 to 16) signaling links that terminate at both ends in common nodes in the CCS network are called

"signaling linksets" in a Signaling System 7 (SS7) network environment.

When a link is brought into service, the function of signaling link management is to perform initial alignment procedure. This consists of running diagnostics or test messages over the signaling links to be sure they can be activated, then changing their state to available-in service (**AVL-IS**). If the signaling link does not pass the tests, or if an error occurs, the signaling link is automatically moved to the available-out of service (**AVL-OOS**). When there is failure, manual intervention may be necessary.

The signaling link management is performed by directing signaling message traffic so as to balance traffic on the remaining links. The following signal link and node abnormalities cause adjustments to be made in load balancing:

- **Signaling Link Failure:** A signaling link may be included in a linkset only if it is in an **AVL-IS** state. It must be removed when it fails and returned to the linkset when it is restored.
- **Link Set Failure:** The signaling linkset has failed only when all signaling links in the set have failed. If there is another linkset available in the route, the traffic from the failed linkset may be diverted to the other available linkset signaling links.
- **Route Failure:** A route is considered failed if a linkset has failed and there is no other linkset in the route to carry the traffic. An alternate route can be selected.
- **Signaling Link Overload:** If a signaling link is overloaded, any route of which it is a part may be overloaded, depending on how well the total traffic load is balanced.

A signaling link may be removed from service by changing the state to the available-manual out of service (**AVL-MOOS**) state by entering `CHG;SLK=LNK-Y;MOOS`.

4.4 SS7 SIGNALING LINK FAULT DETECTION AND RECOVERY

4.4.1 Error Detection

At the end of each signal unit, 16 check bits are provided for error detection. The receiving link node examines the check bits and if consistency is not found between the received check bits and the preceding bits of the signal unit, the signal unit is discarded.

4.4.2 Error Correction

A signal unit that has been transmitted is also retained at the transmitting node until a positive acknowledgement is received. If a negative acknowledgement is received or a time-out occurs, the signal unit is retransmitted.

4.4.3 Signaling Link Error Monitoring

The signal unit error rate monitor is employed while a signaling link is in service and will remove a signaling link from service if a specified error threshold is exceeded. The alignment error rate monitor is employed while a signaling link is in the prove-in state of the initial alignment procedure.

4.4.4 Initial Alignment

The initial alignment is performed before the first time link initialization and after a failed signaling link is restored. The initial alignment consists of a prove-in period and a signaling link translation exchange between the two offices.

4.4.5 Signaling Link Test (SLT)

The on-line signaling link test (SLT) involves automatic communication exchange between two ends of a signaling link. This procedure verifies the physical link assignments and detects looped links or other irregularities. The procedure is used when a signaling link is activated or restored. The signaling link will only be available to carry traffic (in-service) if the test is successful.

The signaling point initiating the tests transmits a test message on the signaling link being tested. The message includes a test pattern, chosen at the discretion of the initiating end and the signaling link code (SLC) of the link being tested. When the message is received, if the SLC identifies the physical link and the office point code (OPC) identifies the signaling point at the other end, a signaling point responds with an acknowledgment message. The test pattern included in the acknowledgment message is identical to the pattern sent in the initial test message.

When the returned test pattern is the same, no further action is taken. If the pattern is different or no acknowledgment is received, the test has failed and the test is repeated once. After a second failure, the link is put out of service. These tests can be performed periodically. (For a description of the improved SLT feature see "Improved Signaling Link Test [SLT] Procedures," Section 4.6.)

4.4.6 Signaling Link Activation

Signaling link activation is the process of preparing a signaling link to carry signaling traffic. If the initial alignment is successful, the signaling link is prepared to carry signaling traffic.

4.4.7 Signaling Link Deactivation

For various reasons, a signaling link may be deactivated or removed from service. When a signaling link is deactivated because of trouble conditions, there are procedures covered in other parts of this document that provide automatic and manual methods of determining the trouble condition and preparing the signaling link for reactivation.

4.4.8 Signaling Link Restoration

There are two types of signaling link restoration: normal and emergency. For normal signaling link restoration, after a signaling link failure is detected, a signaling link alignment is performed including a normal prove-in period. The signaling link is ready for signaling traffic once a successful alignment is completed.

An emergency signaling link restoration is the same as the normal restoration except the prove-in period of the initial alignment is shorter. This restoration procedure is used when no alternate signaling link is available over which to reroute signaling traffic.

4.5 SIGNALING LINK FAILURES

4.5.1 Automatic Changeover

The following is a brief synopsis of the system functions during signaling link failures.

- **Link Restored Within the Time Specified by the T19 Timer.**
 - Error rate monitor detects excessive signal unit errors at the near-end or far-end of the signaling link and a changeover occurs. This means that the messages buffered in the node of the failed signaling link are saved and transmitted over a different signaling link.
 - If the link is activated within the time specified by the T19 timer, traffic changes back to the signaling link.

NOTE: The T19 timer setting defaults to eight minutes.

- **Link Does Not Restore Within the Time Specified by the T19 Timer.**

- Error rate monitor detects excessive signaling errors at the near-end or far-end of the signaling link and a changeover occurs. Messages buffered in the node of the failed signaling link are saved and transmitted over a different signaling link.
- If the link is not activated within the time specified by the T19 timer, it is declared failed. The CN1 requests link node diagnostics.
- After the diagnostics are successfully completed, the signaling link is activated. Signaling traffic is changed back to the signaling link.

NOTE: The T19 timer setting defaults to eight minutes.

- **Link Node Problem Causes Signaling Link to be Declared Failed.**

- Internal link node problem causes the link to be declared failed. Signaling traffic is changed over to alternate signaling links on an emergency basis with buffered messages discarded.
- The signaling link is declared failed and the CN1 requests node diagnostics.
- After the diagnostics are successfully completed, the signaling link is activated. The signaling traffic is changed back to the signaling link.

- **Last Active Signaling Link Fails.**

- During signaling link diagnostics, the link node is declared failed.
- The last active signaling link fails.
- The diagnostics are aborted on the node, the node is repumped, and unconditionally restored. Both signaling links go into emergency activation.
- When the first signaling link proves in and is activated, traffic is routed on this link.

4.6 IMPROVED SIGNALING LINK TEST (SLT) PROCEDURES

4.6.1 Feature Description

The improved signaling link test (SLT) procedure, feature number 99-CP-3072, adds two additional requirements to the SLT procedure:

- (1) The test pattern used in the second signaling test message is the same as the test pattern used in the first message. This allows the first acknowledgment test message to be accepted as a response to the second test message, in effect allowing twice the time for a response to the first signaling message.
- (2) When periodically testing available (in-service) links, the test will even be performed on links which are experiencing transmit or received congestion.

This is a secured feature (SFID=176) and a right-to-use (RTU) fee must be paid to Lucent Technologies before enabling information is provided.

4.6.2 Background

The Signaling Network Systems (SNS) Committee of the Federal Communications Commission (FCC) Network Reliability Council, T1S1.3 provide CCS network architecture evaluations and SS7 protocol enhancements. In the interest of facilitating uniform industry deployment a SNS subgroup prioritized enhancements into two levels. The Improved SLS feature is one of the features in the level two priority group.

4.6.3 Availability

This feature is distributed in the 5E11 software release.

4.6.4 Feature Environment

This feature is provided per switch.

4.6.5 Feature Operation

The signaling link test (SLT) procedure is performed when a signaling link is activated or restored. The link is available to carry signaling traffic (that is, in-service) only if the test is successful. The test is also performed periodically (based on the number of seconds in Timer T2) while links are in-service, even when a link is experiencing transmit or receive congestion.

The signaling point initiating the test transmits a SLT message on the link being tested. This message includes a test pattern chosen at the discretion of the initiating signaling point and the signaling link code (SLC) of the signaling link being tested.

After receiving a SLT message, if the SLC identifies the physical link and the originating point code (OPC) identifies the other end of the link, the receiving signaling point responds with a signaling link acknowledgement message. Otherwise the SLT message is discarded.

The test pattern included in the acknowledgement message is identical to the test pattern received. If the pattern received is different from the one sent, the procedure has failed. It is repeated once. If the second attempt fails the link is put out of service and messages are sent to the management system.

4.6.6 User Operation

The service provider must unlock this secured feature and enable the feature using recent change procedures.

4.6.7 Engineering

4.6.7.1 Hardware Resources

No hardware considerations are associated with this feature.

4.6.7.2 Software Resources

No software considerations are associated with this feature.

4.6.7.3 Transition Considerations

There are no transition considerations associated with this feature.

4.6.8 Interactions and Limitations

There are no interactions or limitations associated with this feature.

4.6.9 Incompatibilities

There are no incompatibilities associated with this feature.

4.6.10 Dependencies

No other features need to be installed or activated.

4.6.11 Isolation Constraints

Not applicable.

4.6.12 Feature Implementation

4.6.12.1 Office Data Administration (ODA) Provisioning

There is no ODA provisioning associated with this feature.

4.6.12.2 Recent Change Provisioning

The service provider must unlock this secured feature and activate the feature using recent change procedures.

Unlock the security lock for the feature by populating Recent Change view 8.22, *Secured Feature Upgrade*:

FIELD	*VALUES
FEATURE ID	176
MODULE	(Office or SM 1-192)
PASSWD	(Provided by Lucent Technologies SFID Administrator)
ACTIVE	Y "Y" - Turns on (unlocks) the feature "N" - Turns off (locks) the feature

Activate the feature using Recent Change view 8.15, *CCS Office Parameters*:

FIELD	*VALUES
IMPROVED SLT	Y "Y" - Turns on (enables) the feature "N" - Turns off (disables) the feature

* See 235-118-2xx, *Recent Change Reference* for detailed information on allowed values.

4.6.12.3 Customer Premises Equipment (CPE)

No CPE is required for this feature.

4.6.13 Maintenance Considerations

Not applicable.

4.6.14 Administration

4.6.14.1 Measurements

This feature does not impact measurements.

4.6.14.2 Billing

This feature does not impact billing.

5. ISDN USER PART (ISUP)

DESCRIPTION

The Integrated Services Digital Network User Part (ISUP) feature provides the 5ESS®-2000 switch with the Signaling System 7 (SS7) protocol requirements for Integrated Services Digital Network (ISDN) basic call processing and other support capabilities. It provides the signaling functions required to support basic bearer services and supplementary services for voice and non-voice applications.

ISUP can be used for the interoffice control of telephone calls emanating from both digital (ISDN) and analog lines. The ISDN callers can be served by an interoffice signaling system other than ISUP, but only the ISUP message repertoire and message structure make the fullest set of ISDN features available on an interoffice basis.

ISUP messages are generated and interpreted by the switches in the Signaling System Network and are carried as the user data in the Message Transfer Part (MTP) message, or in the Signaling Connection Control Part (SCCP) message when SCCP services, beyond the MTP routing services, are required. In summary, ISUP, with the use of the SS7 network services, extends Q.931 (which is a point-to-point network access protocol) over a store-and-forward message switching network.

ISUP provides the basic telephone service defined by Bell Communications Research and T1 Committee for North American Standards. The SS7 ISUP is based on the requirements covered in Bell Communication Research Specification Technical References (TRs).

Signaling functions are performed by ISUP for call setup, call tear down, and trunk maintenance. The most significant advantage of ISUP is the use of SS7 for trunk signaling. The SS7 provides the basis for an almost unlimited variety of trunk signaling for new and improved features. Other advantages of ISUP include improved speed, efficiency of interoffice call setup, and improved fraud prevention.

New SS7 features may be developed with very little feature dependent changes to the ISUP protocol. New messages and parameters can be added to the ISUP protocol without changing existing ones. New message formats allow for definition of mandatory and optional parameters. These parameters are either fixed or variable in length. The longer length of SS7 messages allows each ISUP message to carry more information than Common Channel Interoffice Signaling (CCIS) messages.

USER PERSPECTIVE

The ISUP feature is transparent to the normal telephone user. The switch uses ISUP to perform the signaling functions necessary for call setup, tear down, and trunk maintenance.

The main benefit of ISUP to the non-ISDN user is call setup time. The main benefit to the ISDN user is to have certain necessary supervisory controls to allow the transmission of voice and data, simultaneously.

ISUP CAPABILITY

The basic functions of ISUP are divided into the following areas:

- Call Processing
- Trunk Maintenance
- Data Administration (Translation, Recent Change and Verify)
- Craft Interface
- Measurements (Plant Measurements and Traffic Counts).

5.1 ISUP MESSAGES AND PARAMETERS

5.1.1 ISUP Messages Supported

Table 5.1-1 provides a summary of messages supported by the switch with their corresponding parameters. Some of these parameters are mandatory and some are optional with both fixed and variable lengths. Specifics about each parameter and allowable code values can be found in TR-NWT-000246 — Bell Communications Research Specification of Signaling System 7.

Table 5.1-1 ISUP Messages And Parameters

ISUP MESSAGES
Address Complete Message (ACM) Backward Call Indicator ^a Access Transport Automatic Congestion Control Level Business Group Cause Indicators Information Indicator Optional Backward Call Indicators Unrecognized Parameters ^b User-to-User Information
Answer Message (ANM) Access Transport Backward Call Indicators Business Group Information Indicator Optional Backward Call Indicators User-to-User Information Unrecognized Parameters ^b
Blocking (BLO)
Blocking Acknowledgement (BLA)
Call Progress (CPG) Event Information ^a Access Transport Backward Call Indicators Business Group Cause Indicators Information Indicator Optional Backward Call Indicators User-to-User Information Unrecognized Parameters ^b
Circuit Group Blocking (CGB) Circuit Group Supervision ^a Range and Status ^a
Circuit Group Blocking Acknowledgement (CGBA) Circuit Group Supervision ^a Range and Status ^a
Circuit Group Reset (GRS) ^c Range and Status ^a
Circuit Group Reset Acknowledgement (GRA) ^d
Circuit Group Unblocking (CGU) Circuit Group Supervision ^a Range and Status ^a
Circuit Group Unblocking Acknowledgement (CGUA) Circuit Group Supervision ^a Range and Status ^a
Circuit Query (CQM) Range and Status ^a
Circuit Query Response (CQR) Circuit State Indicator ^a

Range and Status ^a
Circuit Reservation Message (CRM) ^k
Nature of Connection Indicator ^a
Circuit Reservation Acknowledgement (CRA)
Circuit Validation Test Request (CVT)
Circuit Validation Test Response (CVR)
Circuit Group Characteristics ^a
Circuit Identification Name ^a
Circuit Validation Response ^a
CLLI ^a
Confusion (CFN)
Cause Indicators
Continuity (COT)
Continuity Indicators ^a
Continuity Check Request (CCR)
Exit Message (EXM)
Outgoing Trunk Group Number
Facility (FAQ)
Remote Operation Parameter
Facility Reject (FRJ)
Cause Indicators
Facility Indicator
Forward Transfer (FOT) ⁱ
Information (INF)
Information Indicator ^a
Access Transport
Business Group
Calling Party Number
Charge Number
Unrecognized Parameters ^b
User-to-User Information
Information Request (INR)
Information Request Indicators ^a
Backward Network Specific
Unrecognized Parameters ^b
Initial Address Message (IAM) ^k
Called Party Number ^a
Calling Party's Category ^a
Calling Party Presentation Restricted Indicator
Forward Call Indicator ^a
Nature of Connection Indicator ^a
User Service Information ^{a h}
Access Transport
Business Group
Calling Party Number
Carrier Identification ^j
Carrier Selection Information
Charge Number
Generic Address ^f
Generic Digits ^g
Generic Name ^e
Hop Counter Parameter
Information Request Indicators
Jurisdiction Information
Multi-Level Precedence and Preemption
Operator Systems Indicator
Originally Called Number
Originating Line Information
<u>Redirect Capability Parameter</u>
<u>Redirect Counter Parameter</u>
Redirecting Number
Redirection Information

Remote Operation Parameter Service Activation Parameter Transit Network Selection Unrecognized Parameters ^b User-to-User Information
Loop-Back Acknowledgement (LPA)
Pass Along Message (PAM) ⁱ Data
Release (REL) Cause Indicators ^a Access Transport Automatic Congestion Control Level Generic Address Parameter Redirection Number Parameter Service Activation Parameter Remote Operation Parameter Unrecognized Parameters ^b User-to-User Information
Release Complete (RLC)
Reset Circuit (RSC)
Resume (RES) Suspend/Resume Indicators ^a
Suspend (SUS) Suspend/Resume Indicators ^a
Unblocking (UBL)
Unblocking Acknowledgement (UBA)
Unequipped Circuit Identification Code (UCIC)
Notes: a. Mandatory parameters, all other parameters are optional. b. Passed through the switch in an ISUP-to-ISUP connection. c. Sent, and processed on receipt. GRS does not include the status subfield. d. Sent, and processed on receipt. e. Implemented as a special feature. Generated with privacy and availability bits only in a 5ESS [®] -2000 switch OEO. Passed end-to-end in tandem ISUP connection. Only privacy and availability bits are interworked at a 5ESS [®] -2000 switch TEO. f. Passed end-to-end in tandem ISUP connections. Not interworked at a TEO switch. Carries "third party number" outgoing from an OSPA switch. g. Generated in an OSPA office, not understood on input. Passed through as unrecognized on ISUP-to-ISUP connection. Used with "type of digits" field set to "trunk type entering private network" code point for CENTREX. h. Can contain values indicating wide-band calls. i. Not generated, passed through ISUP-to-ISUP, if received. j. Implemented as a secured special feature. k. Starting in 5E13, the priority of IAM and CRM messages can be 0 or 1. See Table 5.1-2.

5.1.2 Priorities For ISUP Messages

Each message sent from the switch is assigned a message priority value (See "MTP Message Priority," Section 2.2.4.2 for an explanation of message priority). The priority values assigned to each ISUP message by the switch are shown in Table 5.1-2.

Table 5.1-2 ISUP Messages Priority

ISUP MESSAGE	PRIORITY
Address Complete (ACM)	2
Answer (ANM)	2
Blocking (BLO)	2
Blocking Acknowledgement (BLA)	2
Call Progress (CPG)	1
Circuit Group Blocking (CGB)	2
Circuit Group Blocking Acknowledgement (CGBA)	2
Circuit Group Reset (GRS)	2
Circuit Group Reset Acknowledgement (GRA)	2
Circuit Group Unblocking (CGU)	2
Circuit Group Unblocking Acknowledgement (CGUA)	2
Circuit Query (CQM)	0
Circuit Query Response (CQR)	0
Circuit Reservation Acknowledgement (CRA)	2
Circuit Reservation Message (CRM) ^a	0 or 1
Circuit Validation Test Request (CVT)	0
Circuit Validation Test Response (CVR)	0
Confusion (CFN)	1
Continuity (COT)	2
Continuity Check Request (CCR)	2
Crankback (CRB)	2
Embedded Pass Along (EPAM)	2
Exit (EXM)	2
Facility Reject (FRJ)	2
Forward Transfer (FOT)	2
Information (INF)	2
Information Request (INR)	2
Initial Address (IAM) ^a	0 or 1
Loop-Back Acknowledgement (LPA)	2
Pass Along (PAM)	2
Release (REL)	2
Release Complete (RLC)	2
Reset Circuit (RSC)	2
Resume (RES)	2
SDN SID/ANI Increment	2
Second Start Dial (SSD)	2
Suspend (SUS)	2
Unblocking (UBL)	2
Unblocking Acknowledgement (UBA)	2
Unequipped Circuit Identification Code (UCIC)	2

Notes:

- a. Starting in 5E13, the priority of the SS7 IAM messages and the SS7 CRM messages sent by the switch can be either **0** or **1**. The default is to send all IAMs and CRMs with a priority level of **1**. However, a recent change option (view 8.15) allows craft personnel to provision the switch to send normal traffic with message priority **0**. When this provisioning is done:

- normal traffic (that not listed in one of the following bullets) has IAM and CRM priorities of **0**,
- the Government Emergency Telecommunications System/High Probability of Completion (GETS/HPC) traffic has IAM priorities of **1** (see Note c. below),
- Multi-Level Precedence and Preemption (MLPP) IAMs marked with a precedence level of **routine** are sent with IAM priorities of **0**, and
- Multi-Level Precedence and Preemption IAMs marked with a precedence level of other than **routine** are sent with IAM priorities of **1**.

This call treatment allows the

- GETS/HPC IAMs and
- MLPP IAMs for calls other than **routine**

to be sent with a higher IAM priority than normal traffic.

See 235-190-115, *Local and Toll System Features* for a detailed description of IAM/CRM priorities used by the Government Emergency Telecommunications Service/High Probability of Completion (GETS/HPC) feature.

- b. The use of HPC Network Capabilities is restricted in the United States and U.S. territories to National Security/Emergency Preparedness (NS/EP) users authorized by the Office of the Manager, National Communications Systems (OMNCS). Telco deployment of these HPC Network Capabilities must be coordinated with the OMNCS at the following address:

Office of the Manager

National Communications System

Attn: GETS Program Office

701 South Courthouse Road

Arlington, VA 22204-2198

email: gets@ncs.gov

5.2 CALL PROCESSING

5.2.1 Call Setup

5.2.1.1 SS7 ISUP Signaling Call Control Messages

Figure 5.2-1 is a simplified diagram showing one example of basic call processing message flow to setup and disconnect an interoffice ISUP call. The calling party disconnects the call first in this example.

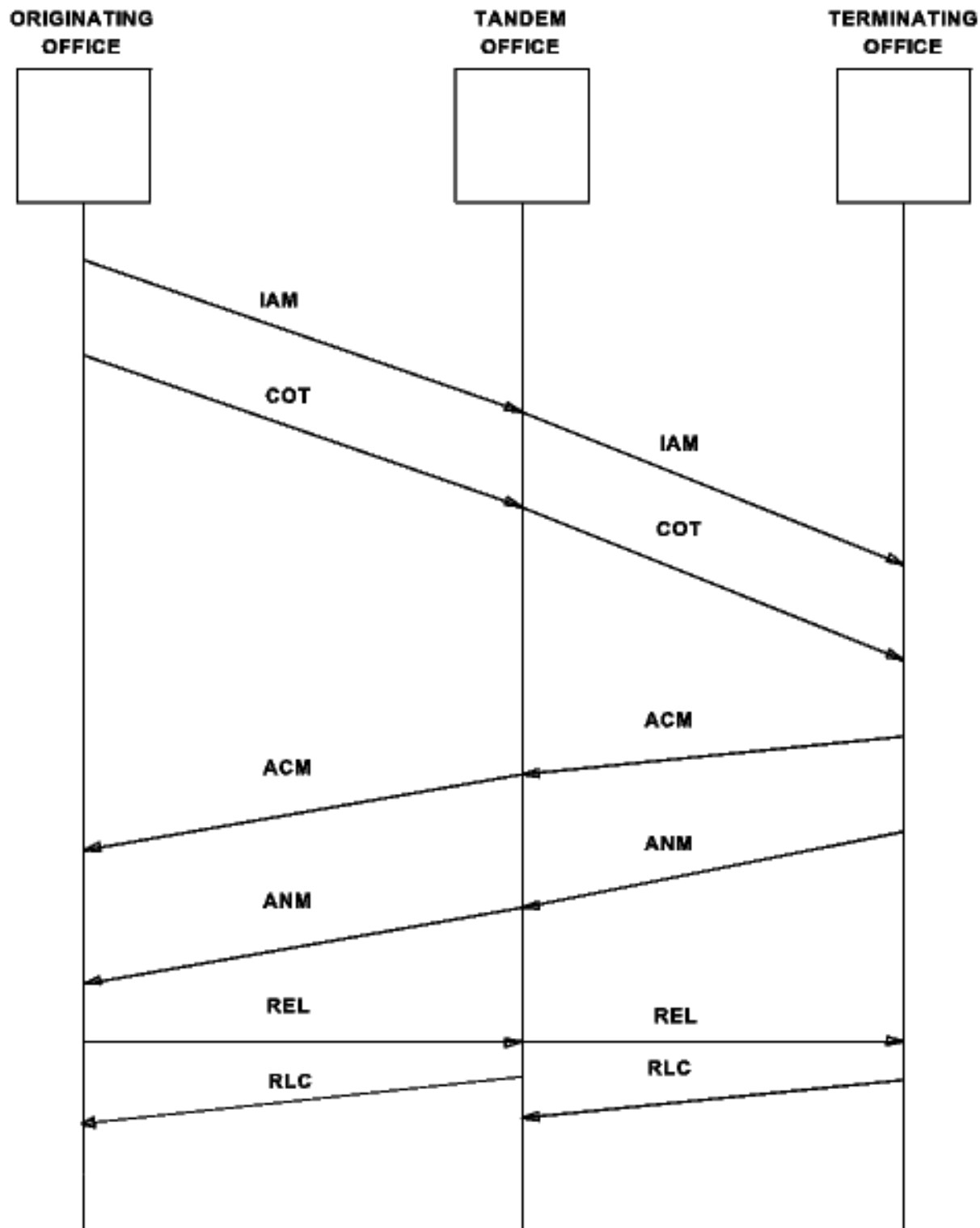


Figure 5.2-1 SS7 ISUP Call Processing Message Flow

The switch uses the SS7 ISUP messages for signaling and supervision between switching offices in the telecommunications network. Each switch supports those messages that are required by other switching offices. Message data parameters are used for defining the type of call, nature of connection, calling party indications, and

other signaling service indicators to assist the switch in call processing.

The call processing software initiates, sets up, supervises, and disconnects basic interoffice SS7 calls. Call processing software also supports the switch features that use SS7 signaling.

Basic call processing involves the sending and receiving of ISUP messages listed in Table 5.1-1. Some of the messages in these tables are similar to CCIS messages for basic call setup and tear down. The ISUP messages are not intended to duplicate the functions of the CCIS messages. The call processing software informs supervision software of the necessary supervision changes when call control messages are received.

5.2.1.2 Originating 5ESS[®]-2000 Switch

After the switch receives the called number from the originating party, routing is determined by internal translations or data base queries. Once the switch determines that a call requires an interoffice connection, it begins the circuit selection process. If the circuit selected for routing the call is an ISUP-supported circuit, the circuit is placed in the busy state. An interoffice call is initiated by the SS7 Initial Address Message (IAM) transmitted for a selected outgoing circuit. This corresponds to sending routing digits through the voice path in a conventional call with inband type signaling.

5.2.1.2.1 Initial Address Message (IAM)

The IAM contains such information as whether the call requires a Continuity test to ensure that the trunk is operational. It also contains the routing digits needed to complete the call, information about the signaling path used thus far in the call connection, bearer capability needed for the call (voice or data), and information about the originating party such as whether the call originated from an ISDN or non-ISDN party. It may optionally contain other parameters containing information about the number to bill for the call and the number of the originating calling party (see Table 5.1-1 for a complete list of the parameters which may be carried in an IAM).

After the originating office sends the IAM, it waits for an indication that the Continuity test passed, if required.

5.2.1.2.2 Continuity Test (COT)

As part of ISUP call processing, continuity checks (also known as voice path assurance test) are performed on circuits to ensure that acceptable transmission occurs through the circuits. This is necessary since signaling and supervision does not occur through the same transmission path. If the continuity check fails, trunk maintenance is called to initiate periodic retest.

For SS7 circuits, verification of continuity is obtained by performing a special inband continuity check. When a circuit is designated as one requiring a continuity check, the nature of connection indicators parameter in the outgoing IAM is coded to indicate that a continuity check is required. The presence of echo suppressors in the circuit hinders the continuity check; therefore, echo suppressors are disabled during the check.

The continuity message is sent immediately following the completion of the continuity check. The continuity message contains the same signaling link selection code and the same circuit identification code as the IAM sent for the outgoing circuit.

If the continuity check fails, the continuity message is populated with the indication "continuity check failed." After this continuity message is sent, the originating exchange attempts to set up the call over a new circuit.

See "Voice Path Assurance Test Considerations," Section 5.9 for more details.

5.2.1.2.3 Address Complete Timer

After sending the IAM, the originating switch begins timing for an indication that the call has reached its final destination which is received in the form of an Address Complete Message (ACM). See Tables 5.5-1 (ADDR

COMP) and 5.6-2 (Tiam) for more details on this timer.

5.2.1.3 Intermediate/Tandem 5ESS®-2000 Switch

When an intermediate switch receives an SS7 IAM, the incoming circuit is identified and marked busy. If the IAM provides sufficient information to enable the exchange to determine that the incoming call requires an outgoing interoffice circuit connection and to select a suitable outgoing circuit, the call is routed even if the received IAM contains optional parameters that the receiving exchange is unable to interpret. (see "Handling Unrecognized Information," Section 5.3.4). The called party address parameter is examined and routing is determined. If the outgoing circuit is SS7, the parameters in the received IAM are examined, modified (if necessary), and passed on in the IAM which is transmitted to the next switch.

5.2.1.3.1 Continuity Test (COT)

If the received IAM indicates that a Continuity Check is to be performed on the incoming circuit, the tandem awaits the inband tone from the preceding switch. Upon receipt of the tone, the tandem exchange returns an inband tone to the preceding switch and begins timer T(ccr,r) for receipt of the COT message (see Table 5.5-1 for details). Upon receipt of the COT message the transit exchange discontinues the inband tone and cancels the timer for the COT message. If COT is required on both the incoming and outgoing circuits at an intermediate exchange, continuity for both circuits must complete successfully prior to the exchange sending the forward exchange a COT message.

If, at an intermediate exchange, continuity fails on the incoming trunk, the trunk is turned over to trunk maintenance for periodic rechecks. If continuity fails on the outgoing trunk, a COT message is sent to the succeeding switch indicating continuity failure and a second attempt is made to establish the call on an alternate outgoing circuit. If the call is rerouted over a second circuit and continuity fails again on the outgoing circuit, a release is sent backward with a cause of "temporary failure."

If the second attempt to establish the call fails for any reason except COT failure, but a successful continuity check is indicated in the continuity message of the incoming circuit, the exchange sends a release message (REL) back to the preceding exchange with a cause parameter indicating the reason for the call failure.

If timer T(ccr,r) times out at the exchange which received the COT request, the exchange will print a Continuity Time-Out (CTO) Machine Detected Interoffice Irregularity (MDII) to the read-only printer. The exchange will then send an REL with cause = "temporary failure" to the preceding exchange.

See "Voice Path Assurance Test Considerations," Section 5.9 for more details.

5.2.1.3.2 Address Complete Timer

After sending the IAM, the intermediate switch begins timing for an indication that the call has reached its final destination which is received in the form of an ACM. See Tables 5.5-1 (ADDR COMP) and 5.6-2 (Tiam) for more information.

5.2.1.4 Terminating 5ESS®-2000 Switch

Upon receipt of the SS7 IAM, the switch checks the IAM for a required Continuity Check on either the incoming circuit or a previous circuit.

5.2.1.4.1 Continuity Check

If the received IAM indicates a Continuity Check is required on either the incoming circuit or a previous circuit, the terminating switch begins timer T(ccr,r) (see Table 5.5-1 for details) to wait for the COT message. If a Continuity Check is to be performed on the incoming circuit, the terminating exchange awaits the inband tone from the

preceding switch and then returns the tone. Upon receipt of the COT message, the terminating exchange discontinues the inband tone and cancels the timer for the COT message. After the continuity check is successful, the called party address is examined and the connection is established.

If timer T(ccr,r) times out at the exchange which received the COT request, the exchange will print a Continuity Time-Out (CTO) Machine Detected Interoffice Irregularity (MDII) to the read-only printer. The exchange will then send an REL with cause = "temporary failure" to the preceding exchange.

See "Voice Path Assurance Test Considerations," Section 5.9 for more details.

5.2.1.4.2 Termination to Called Party

If the called party is a non-ISDN subscriber and is idle, the terminating switch marks the called line busy, applies power ringing to the called line, and connects the incoming trunk to audible ringing to provide for the calling party. An Address Complete Message is then returned to the incoming trunk.

If the called party is an ISDN subscriber and is idle, a Q.931 Setup message is sent to the ISDN terminal. Upon receipt of a Q.931 Alerting message from the ISDN terminal, an Address Complete Message is returned to the incoming trunk and the incoming circuit is connected to audible ringing for the calling party.

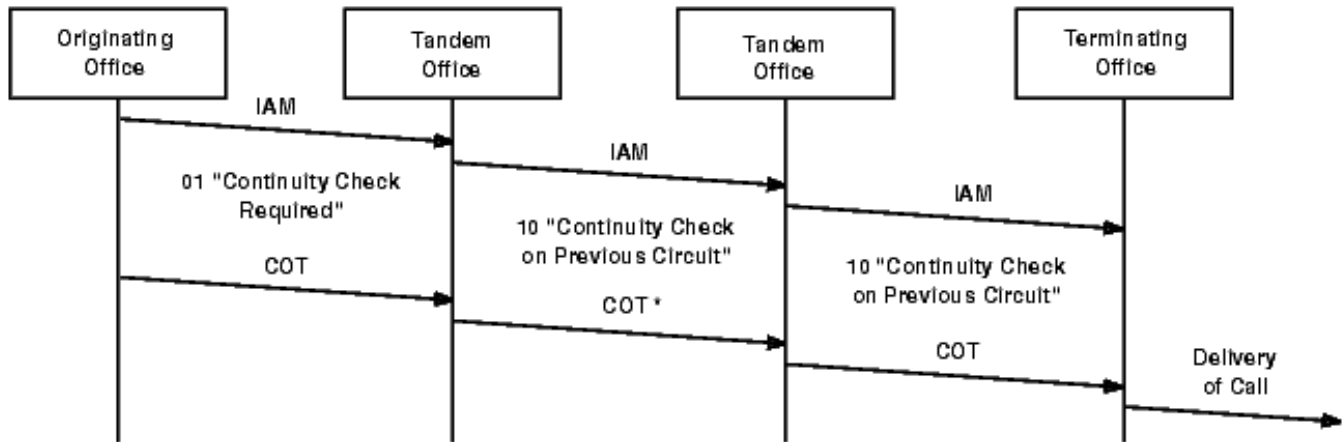
5.2.1.4.3 Network Considerations for VPA Tests

As the calls are sent through the network using ISUP7 trunks, the nature of connection parameter in the IAM is used to signal information about voice path assurance testing and to also tell the forward switch that a COT message is expected from an earlier switch.

For some switches (4ESSTM switch wide band call processing), the code point "VPA on previous circuit" is used as an indication to wait for the COT message, the sending of this message has nothing to do with a VPA test procedure being run. This is, instead, a technique to signal the completion of an internal call setup event.

When a call terminates to a customer at a terminating switch, it is important to wait for the COT message and know that a VPA test procedure is successful before delivering the call to the end customer. Similarly, when a call interworks to an inband signaling trunk at a tandem office, it is important to wait for the COT message before seizing the outgoing trunk to the next office. Not waiting for the COT message in these cases would lead to a false forward signal in case of VPA test failures.

If a call is routed via ISUP7 trunks all the way through the network, then call setup can advance all the way to the terminating switch in parallel with VPA procedures being completed and the COT message coming through as a follow up signal. In this way, call setup is not delayed because of VPA test procedures. This is illustrated in Figure 5.2-2.



* For calls that may interwork to an inband signaling trunk at a tandem office, this event must complete before the outgoing trunk is seized.

Figure 5.2-2 Delay in Interworking or Alerting a Terminating Party with VPA

Switch call processing does not expect to do VPA test procedures for wide band calls. However, if the IAM for a wide band call is received with either "VPA being run on this circuit" or "VPA on previous circuit," then the software waits for the COT message before proceeding with the call setup operations. It then sends the call forward in the network with a nature of connection parameter showing "continuity check not required."

5.2.2 Call Connect

5.2.2.1 Address Complete Message (ACM)

The SS7 Address Complete Message (ACM) is sent from the terminating office to indicate that the address information has been received and call completion steps are to be performed by the terminating office. For voice calls, if called party line failure conditions are detected, the office detecting the failure may provide the failure tones or announcements (see "Unsuccessful Call Setup Procedures," Section 5.3.3). The ACM initiated by the terminating switch contains the mandatory backward call indicator parameter which provides information about the terminating party (see Table 5.1-1).

At the time an ACM is received, the cross-office (transmission) path is completed for voice calls and the calling party then hears audible ringing provided by the terminating switch. (This is not the procedure for a data call - see "Completion Of Transmission Path," Section 5.3.6.)

5.2.2.2 Answer Message (ANM)

When a terminating switch receives an answer indication from the called party, it removes the audible ringing tone from the incoming circuit, if applicable, and cuts through the transmission path to the called party. It then formulates an Answer Message (ANM) and sends it to the preceding switch.

Upon receipt of the ANM, the cross-office connection is complete, the supervisory signal is reported to the switch, and charging is initiated, if required.

5.2.3 Call Release

5.2.3.1 Normal 5ESS®-2000 Switch Call Release

Normal release occurs after call setup if either the calling party, called party, or network initiates a release procedure.

5.2.3.2 Calling Party Initiates a Release

Figure 5.2-3 illustrates the case where the originating party disconnects the call. When ISUP call processing receives an "on-hook" indication from the calling party, it formulates a Release Message (REL) and sends it forward to tear down the call. The procedure for an analog call is the same as for an ISDN call.

5.2.3.2.1 Release Message (REL)

The REL initiated by the calling party identifies the circuit being released and contains the required cause indicator parameter indicating a normal release.

In an intermediate SS7-to-SS7 5ESS®-2000 switch, when the calling party initiates the release, the switch passes the REL message without interpretation and returns an RLC to the preceding switch. Any optional parameters included in the REL message are passed. Each switch sets a long timer [T(rel,l)] and a short timer [T(rel)] to await an acknowledgement from the forward switch in the form of a Release Complete Message (RLC). If timer T(rel) expires before an RLC is received, another REL is sent and T(rel) is restarted. Each switch continues this procedure until an RLC is received, an RSC is sent, and the circuit turned over to trunk maintenance. See Tables 5.5-1 and 5.6-2 for a description of these timers.

5.2.3.2.2 Release Complete Message (RLC)

The RLC message contains no parameters and is sent in response to the REL message.

Upon receipt of a Release Message, each switch in the call connection returns a Release Complete Message (RLC) which indicates that the trunk will be freed up for other traffic.

At the receiving switch, the timers T(rel) and T(rel,l) awaiting the RLC are canceled and the circuit is idled.

5.2.3.3 Non-ISDN Called Party Initiates a Release

When a non-ISDN called party initiates a release, the network initiated suspend/resume operations are applied. The earlier concept of calling party control was required for analog voice calls and normally held up a connection even after the called party released; however, with the called party release function, the switch initiates called party release procedure for analog calls.

Figure 5.2-3 illustrates the use of the **SUS** and the **RES** messages used when the called party goes on-hook and then back off-hook within 10 seconds (note that **SUS** and **RES** messages are only valid when the called party is non-ISDN). This is provided to allow the call connection to remain intact for the 10-second period to guard against false disconnects, and allow for changes in equipment and modes of operation.

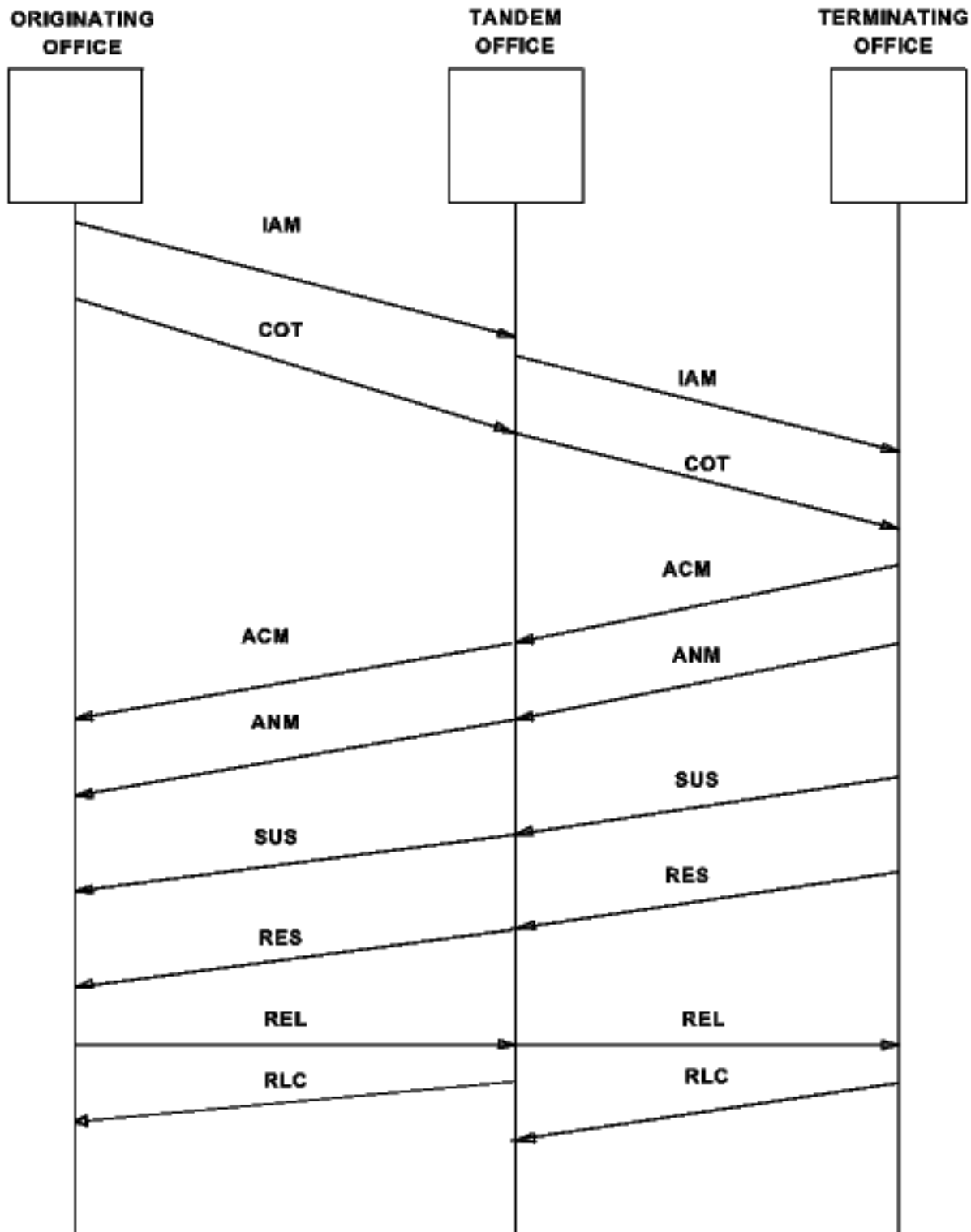


Figure 5.2-3 Delay in Termination of Call - Non-ISDN Called Party Disconnects

5.2.3.4 Suspend Message (SUS)/Resume Message (RES)

5.2.3.4.1 Terminating Switch

The terminating switch only provides the suspend (**SUS**) and resume (**RES**) messages in the talking stage. If the called party is the first to disconnect during a call connection, the terminating switch immediately formulates and sends a suspend message (SUS) for the incoming circuit of the call connection.

When the terminating switch sends the suspend message, it does not idle either the outgoing subscriber line or the incoming circuit. The terminating switch sets a timer to either wait for a Release Message from the calling party or an "off-hook" from the called party indicating that the call has been continued.

If the called party reanswers the phone before an REL is received from the calling party and before the suspend timer expires, the timer is canceled and a Resume message is sent back toward the originating switch.

5.2.3.4.2 Intermediate Switches

Intermediate switches pass any network suspend or resume messages to the connected incoming circuit. In addition, to prevent the trunk from becoming hung, a timer is activated for the SS7 trunk. After the suspend message is sent, if no action occurs on the incoming trunk in a specified period of time, the switch releases the call by sending a Reset Circuit (RSC) message and awaits an acknowledgement via an RLC.

If the incoming circuit is a per-trunk signaling circuit, an on-hook condition is provided when a **SUS** message is received. The **RES** message results in an off-hook indication on per-trunk signaling circuits.

5.3 BASIC CALL SETUP ENHANCEMENTS

5.3.1 Fast Connect

At the originating SS7 5ESS[®]-2000 switch, the ANM is expected after the ACM. If the call is answered by an automatic terminal, an ACM may not be required by the terminating office. The SS7 answer message may be received without the ACM.

If an ANM is received at a tandem without having previously received an ACM, only an ANM is sent. If the incoming circuit is SS7 supported, the tandem formulates and sends an ANM for the incoming circuit. If the backward call indicator parameter is received in the ANM, this parameter is included in any outgoing ANM. The parameters included in this ANM and their coding are the same as in the received ANM, except for the ISUP protocol control indicator fields in the backward call indicator parameter. These bits are coded to reflect any changes resulting from the characteristics of the forward connection.

5.3.2 Mapping Cause Values At A Tandem Exchange

5.3.2.1 Background

In the 5E5 software release, the cause indicator parameter is not preserved through a switch. The location field within the cause indicator parameter is hard-coded to "user" before being sent out of the switch and cause values may not be passed through the switch unchanged.

In 5E6, the cause transparency rule has been implemented. This rule states that the received cause indicator parameter should be passed through a switch unchanged. Although this is the general rule, there are exceptions.

NOTE: In the 5E6 software release, the cause indicator parameter is only supported in the Release (REL) Message.

In 5E7, the cause indicator parameter is supported in the REL, the Address Complete Message (ACM), and the Call Progress (CPG) Message. New exceptions to the cause/location transparency rule have also been added, in addition to the 5E6 exceptions.

5.3.2.2 5E6 Exceptions to Cause/Location Transparency Rule

Before sending a message with a cause indicator parameter across a network boundary (that is from a toll network to an LEC network or from an LEC network to a Toll network), the location field within the parameter may be recoded. These recodings are documented in "ISUP Network Interconnect," Section 10 in this document. Refer to Figures 10-17 and 10-18 in "Call Release Message Flow," Section 10.5.11.

5.3.2.3 5E7 Exceptions to Cause/Location Transparency Rule

A switch running the 5E7 software release will have the same cause/location transparency rule exceptions as described previously. The following exceptions were added for the 5E7 software release:

- (1) Cause values in the protocol error class other than "recovery from timer expiry" (102) are changed to "temporary failure" (41).

NOTE: Each cause value belongs to a class. The class is determined by the three high order bits of the cause value. For example, a cause value of "message type nonexistent or not implemented" (97) would be represented by 110 0001 in binary. The class of this cause is 110 (binary). This is the protocol error class. All causes between 110 0000 (96 decimal) and 110 1111 (111 decimal) are in the protocol error class.

- (2) A cause value of "resource unavailable - unspecified" (47) is recoded to "temporary failure" (41).

- (3) A location value of "local interface controlled by this signaling link" will be recoded to "local local network" if the associated ISUP circuit is not connected to an interexchange carrier (IEC).

5.3.3 Unsuccessful Call Setup Procedures

5.3.3.1 Unsuccessful Call Setup (5E6 Software Release)

5.3.3.1.1 Unsuccessful Call Setup (5E6 Software Release) Introduction

If the connection cannot be completed or maintained during call setup, a tone, announcement, or an REL is returned. An REL, when returned, contains a cause value that identifies the reason for the call failure. If the REL is returned before the ACM is received, then all cause values will be regarded as failures, including the following "normal" values:

- Normal clearing
- Normal, unspecified
- Interworking, unspecified.

The REL received after the ACM does not initiate call failure procedures, but initiates normal call clearing procedures, as discussed previously.

Because the announcements are not consistent, an REL returned by one office may trigger an undesired announcement in another office if interworking is encountered or the originating access is non-ISDN. It is assumed for network interconnect purposes, only busy and reorder tones are available at all offices. If a network owner thinks that it is necessary to have an announcement rather than a tone, the announcement can be provided. However, within a particular network, the announcement may be available at most (if not all) offices. If the announcements are the same, the REL returned from a preceding office provides the required inband announcement. For RELs that cross network boundaries, the type of announcement provided cannot be guaranteed.

5.3.3.1.2 Returning a Release Message

An REL is returned only when the call failure reason can be sufficiently identified by one of the available cause values. For special situations, the failing office needs to provide the necessary inband tone or announcement.

If the incoming circuit uses a non-SS7 protocol that cannot convey the call failure reason, the office provides the appropriate tone or announcement.

If the initial address message (IAM) for the call indicates "unrestricted digital information" or "restricted digital information" (that is, a data call) in the user service information parameter, a release is returned.

If the incoming circuit uses SS7 signaling, an REL is sent to the preceding office with the appropriate cause based on the failure.

After a release complete message (RLC) is returned from the preceding office, the circuit is changed to the idle condition.

5.3.3.2 Returning an Inband Indication (Tone or Announcement)

If the office returning the inband indication is the same office that initiates the release, the call may be routed to an automatic intercept system to provide a specialized announcement.

If the office returning the inband indication is not the initiating office, the call failure reason is identified by the cause value in the REL received from the succeeding office. Table 5.3-3 relates the REL cause value to the tones and announcements returned as a result of the release.

Before an inband indication can be returned on an incoming circuit, the office must ensure that the transmission path has been completed at the preceding office.

If the incoming circuit uses SS7 signaling and the ACM has not been returned for the call, the ACM message is returned at this time. The ACM has the backward call indicator parameter coded "interworking encountered" to ensure completion of the transmission path and to cause a Q.931 progress message to be returned if the originating access is ISDN.

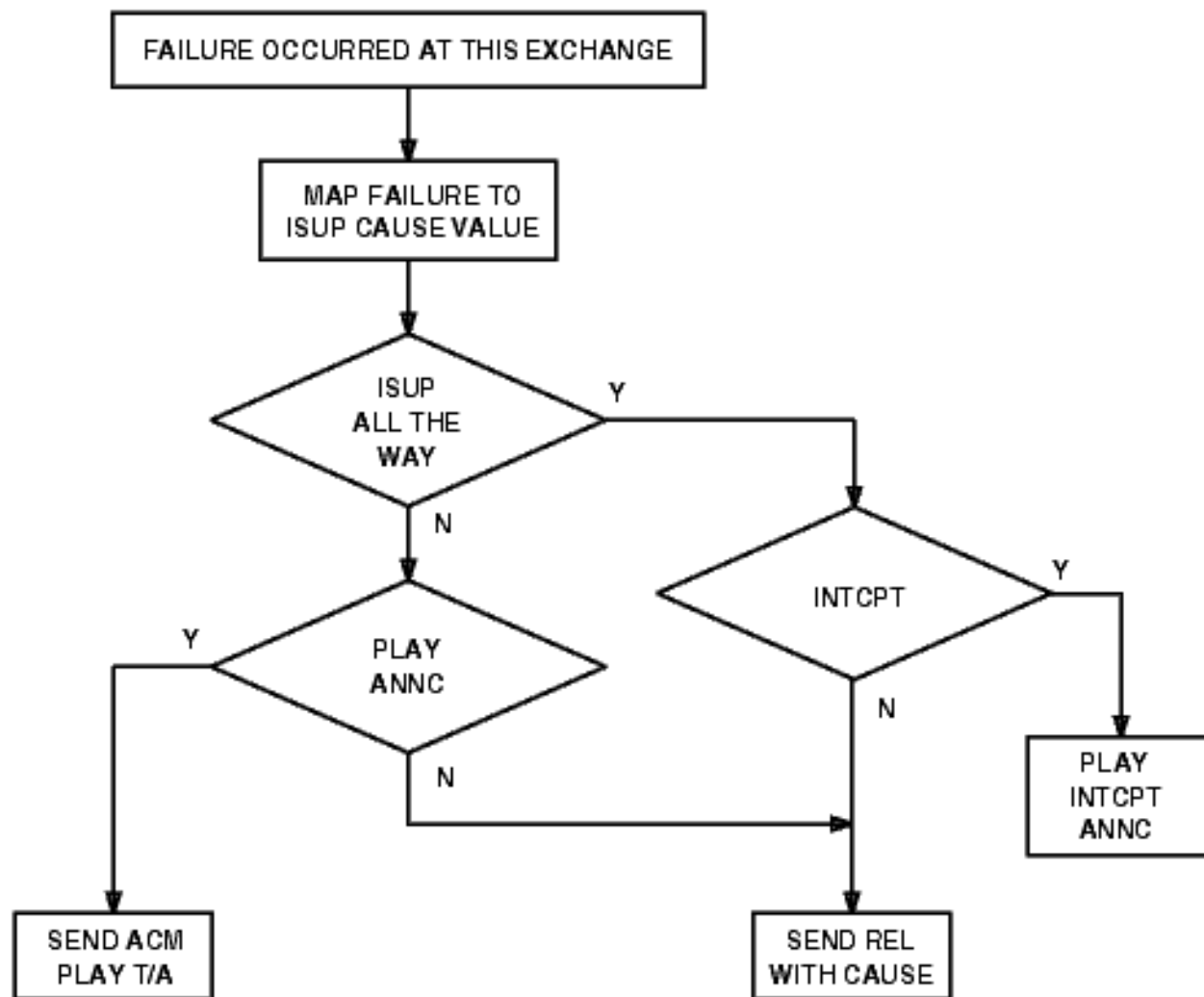
If the incoming circuit uses non-SS7 signaling, appropriate action, such as signaling off-hook is taken.

The appropriate tone or announcement is connected to the incoming circuit. If a time-out period is associated with the tone or announcement and the period is exceeded, the connection is released.

5.3.3.2.1 Action at the Originating End Office When Receiving REL

If the originating access is ISDN, the cause value in the REL is interworked with the Q.931 disconnect message as specified in "ISDN User-Network Interface," Section 9.

For non-ISDN access or ISDN "speech" or "3.1 kHz audio" calls, the office provides the appropriate tone or announcement based on the received cause. Figure 5.3-1 describes the handling of unsuccessful calls in the 5E6 software release.



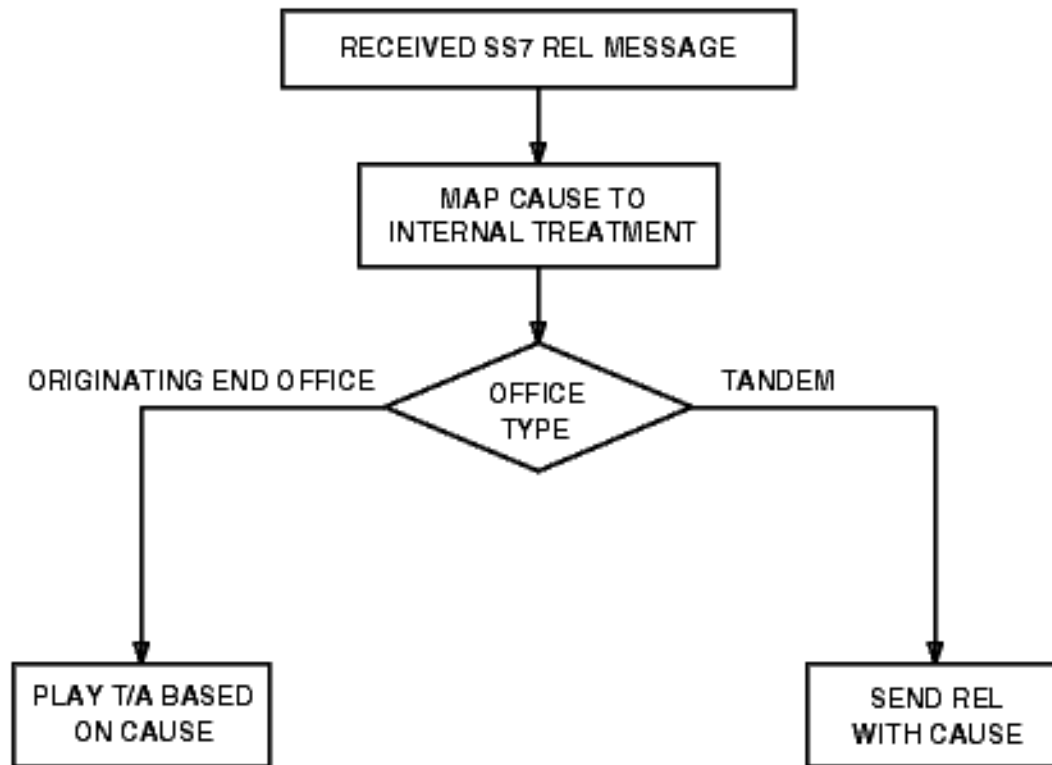


Figure 5.3-1 5E6 Call Setup Failure

5.3.3.3 Unsuccessful Call Setup (5E7)

In previous software releases, the switch, as terminating exchanges, did not have the capability to provide call failure treatment based on the failure condition and the setting of the forward call indicator parameter. The procedure at the terminating/tandem exchanges encountering call failure conditions, as well as association of the received cause indicator parameter with inband treatment at the originating/tandem exchanges, are now provided in alignment with Bellcore requirements. Figure 5.3-2 and Tables 5.3-2 and 5.3-3 describe the handling of unsuccessful calls.

5.3.3.3.1 Failure Encountered at the Terminating Exchange

The following procedures apply to all calls; that is, calls with terminating access ISDN and non-ISDN.

Certain failure conditions may occur at the terminating exchange after the receipt of the IAM and before sending of the ACM.

5.3.3.3.1.1 Intercept Treatment

If a call failure event associated with one of the cause values "destination out of order (27)," "unallocated number (1)," or "number changed (22)" is encountered at the terminating exchange, the following procedures apply.

If the information transfer capability in the user service information parameter in the received IAM indicates that the bearer capability is "speech" or "3.1 kHz audio," an inband tone or announcement is provided either by the terminating exchange or by a remote automatic intercept system (AIS). For the three events specified previously, an REL is not sent for the incoming circuit if the information transfer capability of the calling party is "3.1 kHz audio" or "speech," for either ISDN and non-ISDN originating access.

If the inband tone or announcement is to be provided by the terminating exchange, the exchange returns an ACM for the incoming circuit and then connects the incoming circuit to an appropriate tone or announcement.

If the call is routed to a remote announcement (AIS), an ACM is returned for the incoming circuit.

If the user service information indicates that the information transfer capability is "unrestricted digital information" or "restricted digital information," no inband tone or announcement is provided.

5.3.3.3.1.2 Bearer Capability Not Supported at the Terminating Interface

Upon receipt of the IAM, the terminating exchange determines if the called line can receive a call of requested user service information (bearer capability). If the requested user service information cannot be supported, the exchange sends an SS7 REL for the incoming circuit. The cause value is "bearer capability not implemented (65)."

5.3.3.3.1.3 Other Call Failure Treatments

If the call cannot be routed to its destination at the terminating exchange for failure conditions other than those associated with cause values "destination out of order (27)," "number changed (22)," "unallocated number (1)," "user busy (17)," and "bearer capability not implemented (65)," the exchange uses the following procedures:

- *Originating Access Non-ISDN*
 - If the calling party is non-ISDN [that is, the ISDN access indicator bit of the forward call indicator (FCI) parameter in the IAM received is coded "originating access non-ISDN"] and if the information transfer capability in the user service information parameter is "3.1 kHz audio" or "speech," the exchange provides treatment which is determined by the setting of the ISUP indicator bit in the FCI parameter in the IAM, unless a specialized tone/announcement (for example, network management controls, EA1-EA7, SP1, and SP2) is to be provided for the call failure event. There are two recent changeable per-office indicators (See Table 5.3-1). The first indicator, LEC ANNC, applies when the ISUP indicator is set to ISUP used all the way. The second indicator, LEC IW REL applies for ISUP not used all the way. The treatment to be provided is determined in Table 5.3-2 and Table 5.3-3 . If tone or announcement is to be played at this office for this failure event, an ACM is returned for the incoming circuit.
 - If the originating access is non-ISDN and the user service information parameter in the IAM indicates "unrestricted digital information" or "restricted digital information," an REL is returned for the incoming circuit. The REL contains a cause value associated with the failure condition.
- *Originating Access ISDN*
 - If the originating access is ISDN and the user service information parameter in the IAM indicates "3.1 kHz audio" or "speech," an REL is returned for the incoming circuit, with the following exception. If a specialized tone/announcement is to be provided for the call failure event, the terminating exchange may provide the tone/announcement or route the call to an AIS, and send an ACM for the incoming circuit.
 - If the originating access is ISDN and the user service information parameter in the IAM indicates "unrestricted digital information" or "restricted digital information," an REL is returned for the incoming circuit. The REL contains a cause value associated with the failure condition.

5.3.3.3.1.4 Terminating Interface Busy

If the terminating exchange determines that a non-ISDN called line or a called ISDN interface is busy, the procedure depends on the forward call indicator (FCI) parameter received in the IAM.

If the interworking bit in the FCI parameter is set to "no interworking encountered," then the terminating exchange returns an REL for the incoming circuit.

If the interworking bit in the FCI parameter is set to "interworking encountered," then the procedure at the terminating exchange depends on the setting of a recent changeable office option, "Busy Annc." The default setting of the option is to send an REL for the incoming circuit ("Send REL"). The other setting of the option is to provide busy tone from the terminating exchange after returning an ACM for the call ("Play T/A").

If the option "Busy Annc" is set to "Send REL," then the terminating exchange returns an REL for the incoming circuit.

5.3.3.3.2 Recent Changeable Options

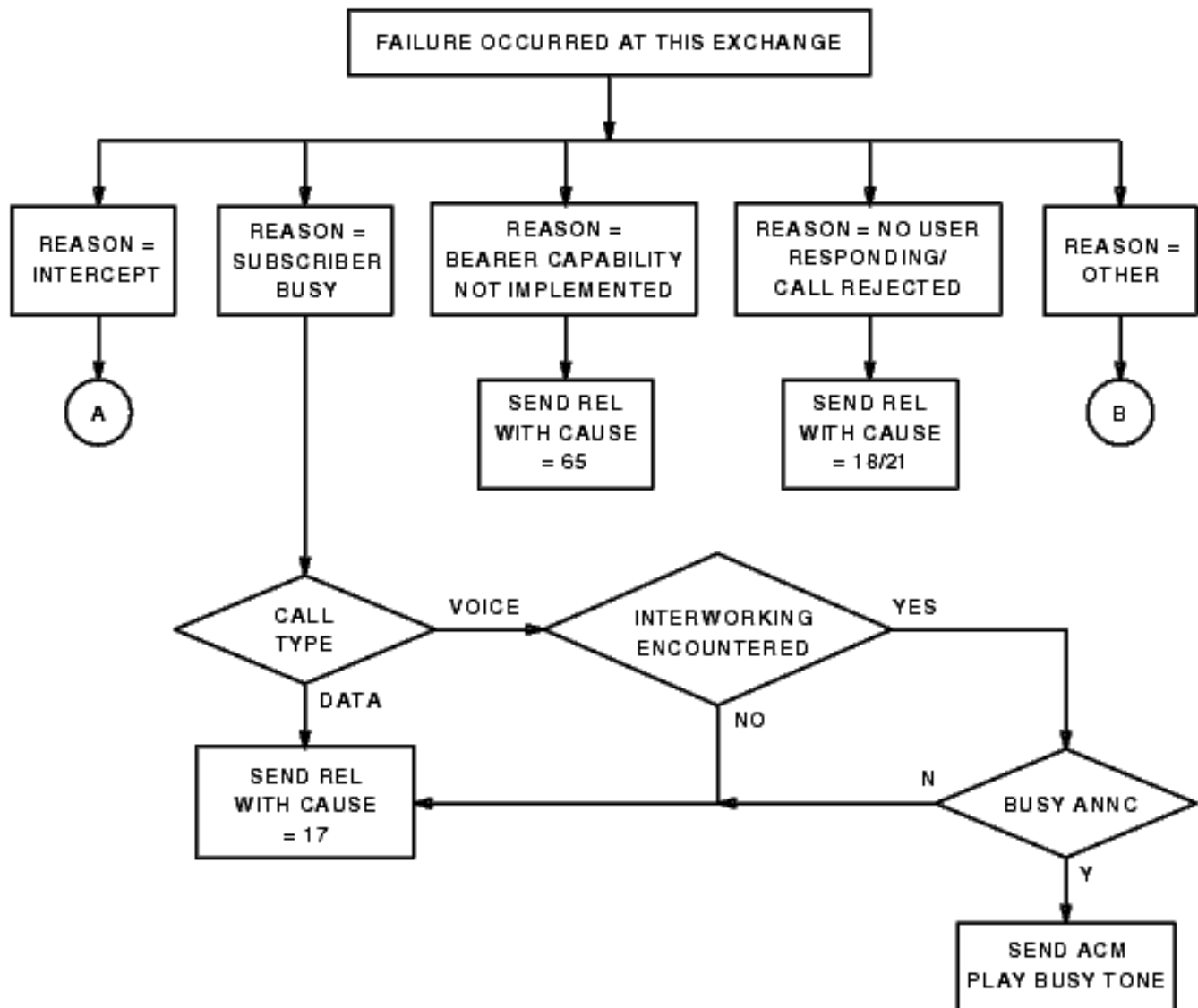
There are five recent changeable indicators applicable to local switches for unsuccessful call setup procedures:

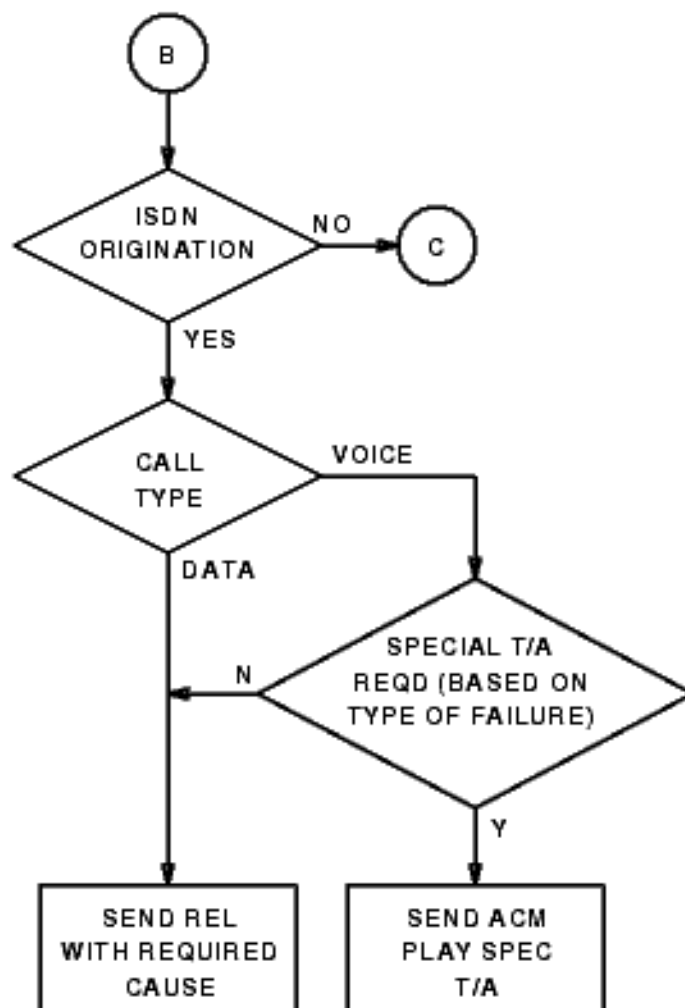
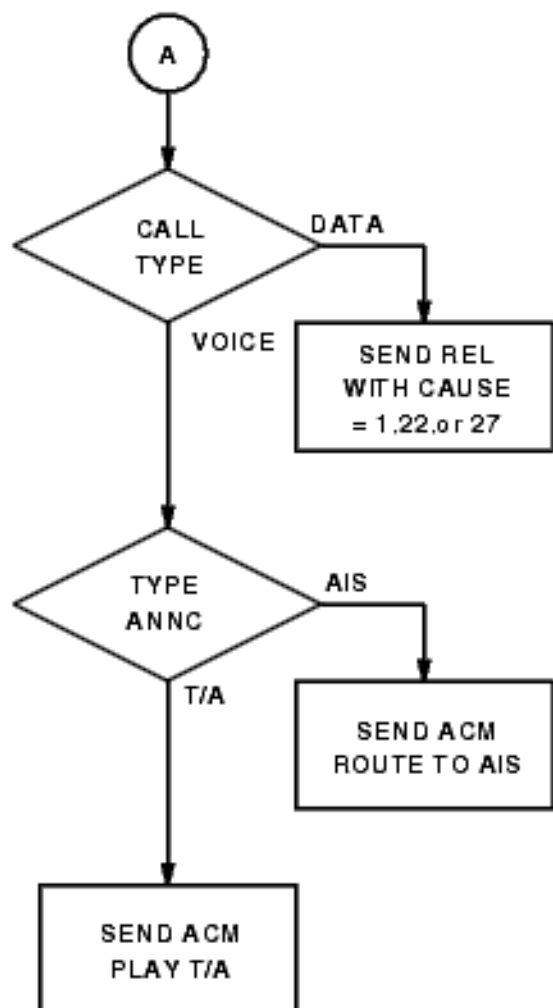
- LEC ANNC (Per Office Indicator)
- LEC IW REL (Per Office Indicator)
- BUSY ANNC (Per Office Indicator)
- NI ANNC (Internetwork Circuit Group Indicator)
- NI IW REL (Internetwork Circuit Group Indicator)

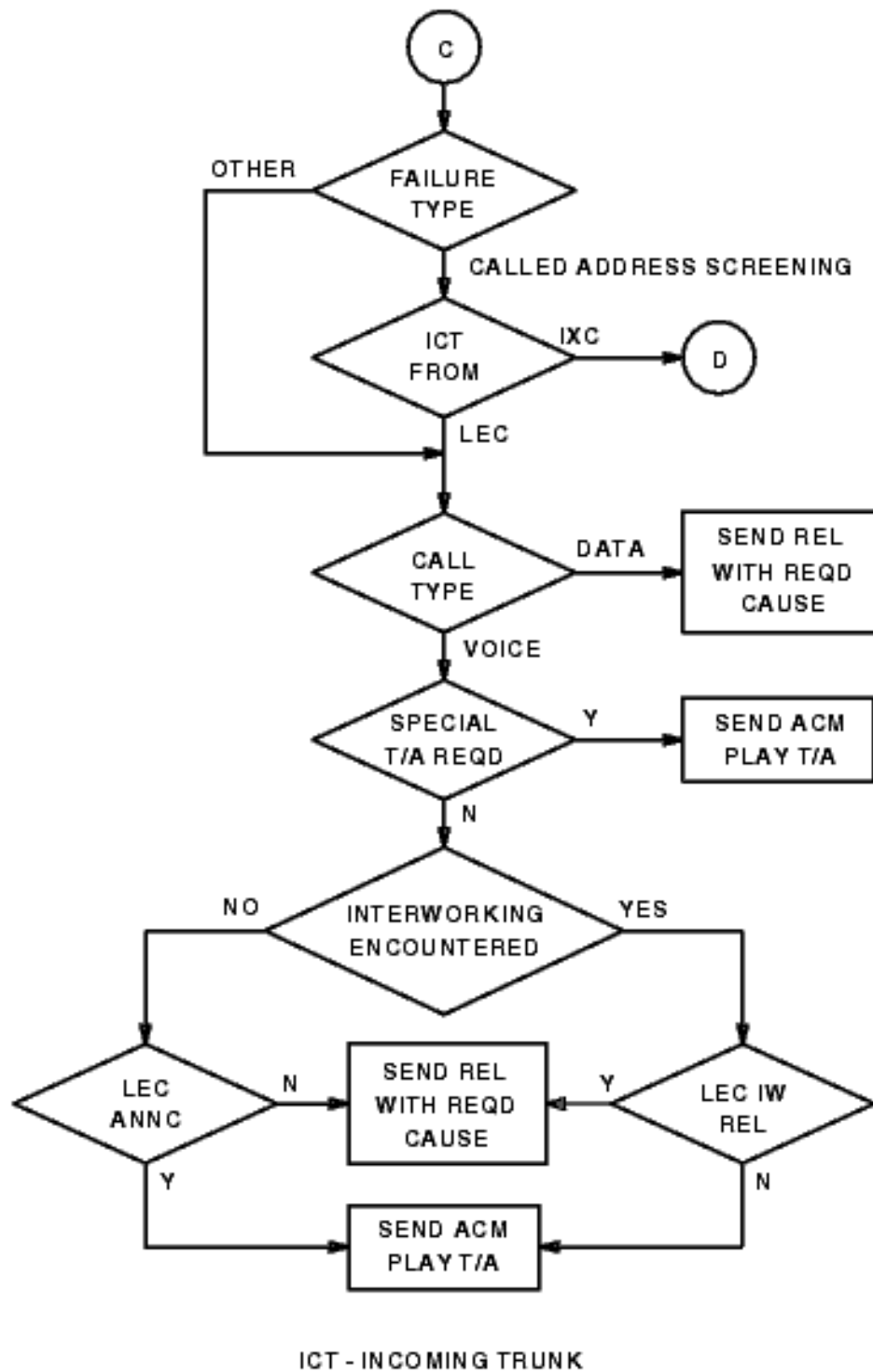
These indicators are only applicable to non-ISDN originated "speech" or "3.1 kHz audio" calls. Based on the setting of the appropriate indicator, the exchange will either provide a tone/announcement or return an REL message to the preceding exchange. Table 5.3-1 and Figure 5.3-2 describe how the five indicators are used.

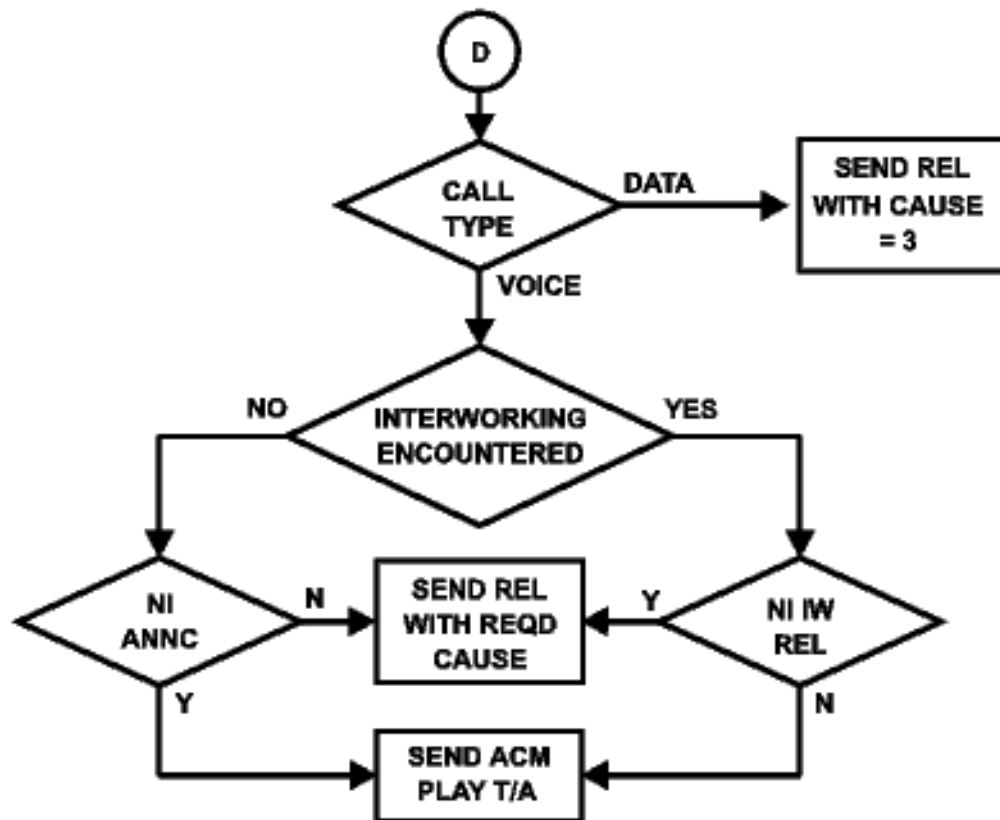
Table 5.3-1 Call Failure Treatment For Non-ISDN Originated Calls

CHARACTERISTICS OF THE CALL	RECENT CHANGE VIEW	RECENT CHANGEABLE INDICATOR	INDICATOR SETTING	SWITCH ACTION
ISUP used all the way ^a	8.15	LEC ANNC	Y	Provide T/A
			N ^b	Return REL
ISUP not used all the way ^a	8.15	LEC IW REL	Y	Return REL
			N ^b	Provide T/A
Interworking encountered ^c	8.15	BUSY ANNC	Y	Provide busy tone
			N ^b	Return REL
ISUP used all the way ^a	5.1	NI ANNC	Y	Provide T/A
			N ^b	Return REL
ISUP not used all the way ^a	5.1	NI IW REL	Y	Return REL
			N ^b	Provide T/A
Notes:				
a. Setting of ISUP Indicator in the FCI parameter.				
b. Default setting of the option.				
c. Setting of Interworking bit in FCI parameter.				









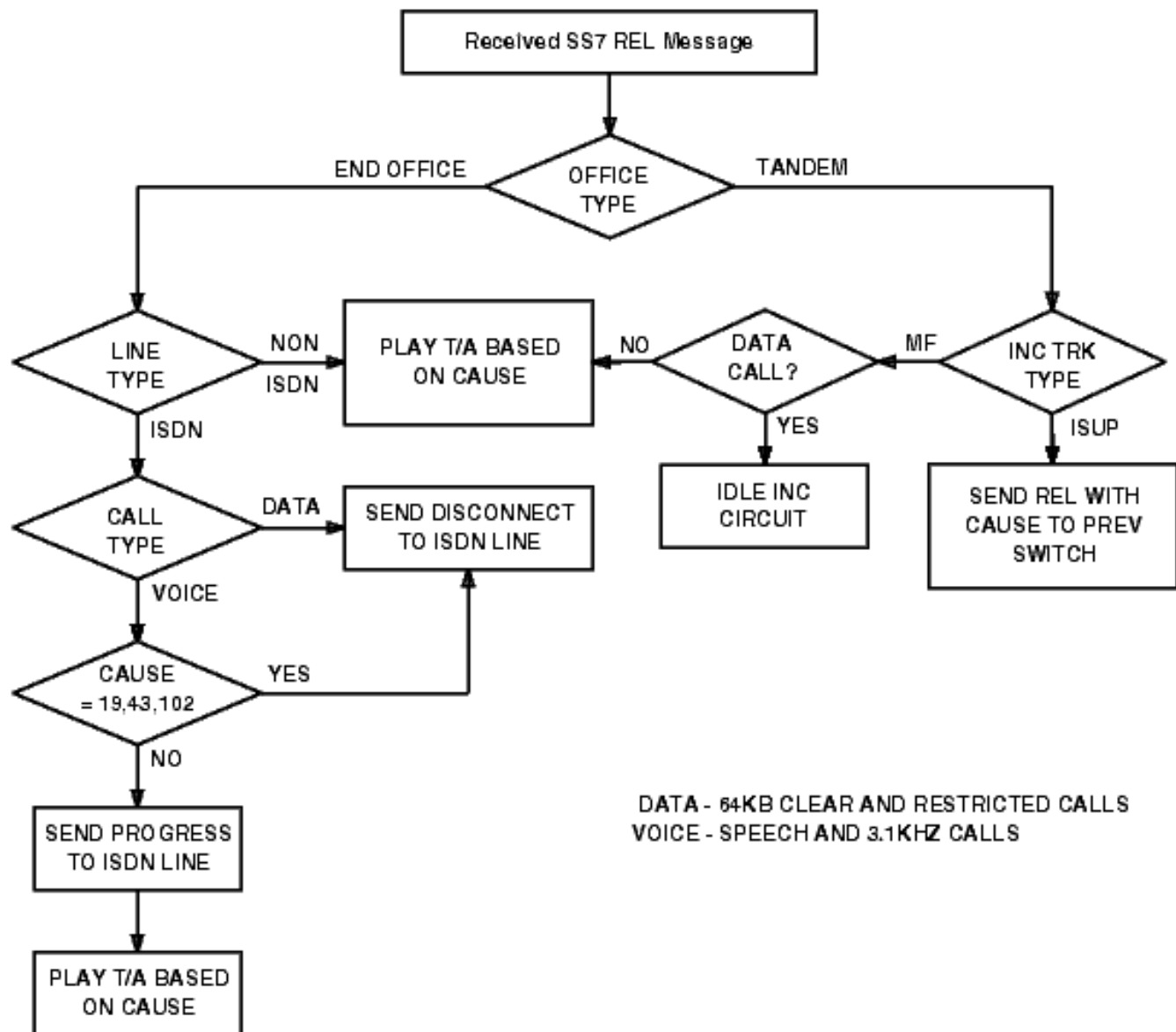


Figure 5.3-2 Call Setup Failure

Table 5.3-2 Release Message Cause Coding For Call Failure

FAILURE CONDITION	CAUSE VALUE	
No Circuit Available	No Circuit Available	34
Switching Equipment Congestion	Switching Equipment Congestion	42
Automatic Repeat Attempt Failed ^a	Temporary Failure	41
Expiration of Timer T_{IAM}	Temporary Failure	41
Expiration of Timer T_{CRM}^b	Temporary Failure	41
Expiration of Timer $T_{CCR,r}$	Temporary Failure	41
Expiration of Timer T_{CRA}^b	Temporary Failure	41
No Wink Returned	Temporary Failure	41
Off-Hook Instead of Wink ^b	Temporary Failure	41
Preemption	Preemption	45
Unknown Carrier Code	No Route to Specified Transit Network	2
Unknown/Invalid Circuit Code	No Route to Destination	3

Invalid CDPN Nature of Address	No Route to Destination	3
Unknown CDPN Nature of Address	Invalid Protocol Contents	100
Incomplete Address Received	Address Incomplete	28
Non-Subtending Called Party	No Route to Destination	3
Vacant Code	No Route to Destination	3
Vacant Number	Unallocated Number	1 ^c
LRN Routed Call to Unallocated DN	Misrouted Call to Ported Number	26
Number Changed	Number Changed	22 ^c
ISUP Hop Counter Exchange Routing Error	Exchange Routing Error	25
Destination Out of Service	Destination Out of Service	27 ^c
Unsupported Bearer Capability	Bearer Capability Not Implemented	65
Incompatible Destination	Incompatible Destination	88
Incoming Call Restriction	No Circuit Available	34
User Busy	User Busy	17
No User Responding	No User Responding ^d	18
Call Rejected	Call Rejected ^d	21
No Answer From ISDN User	No Answer From ISDN User ^d	19
Intra-Office Failure	Temporary Failure	41
Intranetwork Failure	Temporary Failure	41
Internetwork Failure	Temporary Failure	41
Unsupported Bearer Capability	Bearer Capability Not Authorized	57
Terminal Does Not Belong To the Required	Unallocated Destination Number	23
Terminal Group ^e		
Received mbgid Could Not Be Translated Into a tgid Value ^e	Unknown Business Group	24
Restriction Screening Error ^e	Call Blocked Due To Group Restrictions	54
Wideband 384 kb/s call not on Channels 1, 7, 13, or 19	Invalid Protocol Contents	100
Wideband calls on Different Trunks Groups on Same Facility	Invalid Protocol Contents	100
Wideband Call Failed Due to Path Hunt Blocking	Temporary Failure	41
Reject Incoming Wideband Test Call	Protocol Error, Unspecified	111
Notes:		
a. Failure after second attempt due to dual seizure; receipt of blocking, reset circuit, or unequipped circuit identification code message; continuity check failure; or receipt of an unreasonable message.		
b. Interworking with inband signaling only.		
c. Only for data calls.		
d. Interworking with Q.931 only.		
e. Only sent for Multi-switch Business Group (MBG) calls.		

Table 5.3-3 Tone and Announcement From Cause Coding

CAUSE VALUE		DOMESTIC TREATMENT ^{a b}
1	Unallocated Number	VCA
2	No Route to Specified Transit Network	VCA
3	No Route to Destination	VCA
4	Send Special Information Tone	T
16	Normal Release	T
17	User Busy	BT
18	No User Responding	Audible
21	Call Rejected	Audible
22	Number Changed	VCA
23	Unallocated Destination Number	T ^c
24	Unknown Business Group	T ^c
25	Exchange Routing Error	T
26	Misrouted Call to Ported Number	T ^d
27	Destination Out of Service	SC
28	Address Incomplete	VCA
31	Normal, Unspecified	T

34	No Circuit Available	NCA
38	Network Out of Order	NCC
41	Temporary Failure	T
41	Temporary Failure(Location = User)	Busy
42	Switching Equipment Congestion	SC
45	Preemption	T
47	Resource Unavailable	Ckt Grp Congestion
54	Call Blocked Due To Group Restrictions	T c
65	Bearer Capability Not Implemented	VCA
100	Parameter w/Invalid Coding	SC
111	Protocol Error, Unspecified	SC
127	Interworking, Unspecified	T
1-33	Others	T
34-47	Others	SC
48-95	Others	VCA
96-111	Others	SC
112-127	Others	T

Notes:

a. Reorder tone may be provided in place of any announcement.

b. Definitions of terms in this table are as follows:

- Busy tone (BT) (60 IPM)
- Unable to complete (VCA)
- Call did not go through (ROA)
- No circuit to carrier (NCC)
- Reorder (T) (120 IPM)
- Switch Congestion (SC)
- All circuits busy (NCA)

c. Treatment optioned on Recent Change View 12.21.

d. Treatment optioned on Recent Change View 10.1:

set to PFXREQD for 5E11 and 5E12,

set to MISRLRN for 5E13.

5.3.3.3 Unsupported Release Cause Values

Table 5.3-4 contains the cause values not explicitly supported by the switch and their interpretations, if received.

Table 5.3-4 Unsupported Call Release Causes

RECEIVED CAUSES	CAUSES INTERPRETATION
(5-15), (20), (29-30)	(31) Normal - Unspecified
(32-33), (35-37), (39-40), (46)	(47) Resource Unavailable
(48-53), (55-56), (59-62)	(63) Service/Option Not Available
	- Unspecified
(64), (67-69), (71-78)	(79) Service or Option Not Implemented - Unspecified
(80), (82-87), (89-94)	(95) Invalid Message
(96), (98), (101), (103-110)	(111) Protocol Error, Unspecified

(112-126) and Any Other Undefined Causes	(127) Interworking, Unspecified

5.3.4 Handling Unrecognized Information

Any information that is not specified in the protocol specification is interpreted as unrecognized. Special requirements may allow these rules to be suspended. Unimplemented messages, parameters, or fields are interpreted as unrecognized.

5.3.4.1 Confusion Message (CFN)

The purpose of the CFN message is to indicate that unrecognized signaling information has been received at an exchange. Unrecognized signaling information refers to those messages of the ISUP protocol that an exchange has not implemented.

Any standardized message that is implemented at the receiving exchange is considered "recognized." If such a message is received intra-LATA and it is implemented at the receiving exchange, it is treated as a recognized message. Any message not defined as recognized is considered unrecognized, see "Handling Unrecognized Information," Section 5.3.4. Unexpected messages are messages recognized by the exchange but are received out of sequence. Receipt of such messages does not trigger the generation of the confusion message. In such cases, current procedures for handling unexpected messages are followed.

The generation of the confusion message is determined by the setting of a recent changeable switch option for each trunk group. The default setting of this option is to generate the message. See Table 5.5-1, CFN RSTRCT, for more details.

If any message is received at an exchange that is not implemented by that exchange, the message is discarded and a confusion message is returned to the exchange that sent the unrecognized message. The confusion message includes the cause indicator parameter with a cause value of "message type non-existent or not implemented," and location of "local local network," followed by a diagnostic field which contains the message type of the unrecognized message. For an equipped trunk, the generation of the confusion message is independent of the maintenance or busy/idle state of that trunk.

A confusion message is not sent in response to a received confusion message. For multiple occurrences of unrecognized messages, a confusion message is sent for each occurrence. The confusion message is returned immediately without interfering with normal call processing.

If a recognized message contains one or more unrecognized optional parameters, or mandatory or optional parameters containing unrecognized values, the procedures in "Unrecognized Parameter Values," Section 5.3.4.3 are followed. No confusion message is returned.

5.3.4.2 Unrecognized Parameters

5.3.4.2.1 Parameter Passing

Some messages passing through the network have parameters required by switches other than the switch. Messages with parameters that are not used by the switch for call processing may be allowed to pass. This allows future parameters to be added to the protocol without modification to each SS7 5ESS®-2000 switch.

If unrecognized optional parameters are received within the IAM, ACM, ANM, CPG, REL, information request message (INR) and information message (INF), the procedures taken depend on whether or not the receiving exchange is the destination exchange for the message. For ISUP-ISUP connections, unrecognized parameters are passed through the switch without modification.

The operation performed at the receiving exchange is described as follows:

- If the receiving exchange is not the destination exchange of the message, the unrecognized optional parameters are passed transparently without any modification to the succeeding/preceding exchange.
- If all of the unrecognized parameters cannot be passed (for example, because total message size exceeds 272 bytes), some unrecognized optional parameters may be dropped. If any unrecognized optional parameters need to be dropped, the unrecognized parameter received last in the message is dropped first. If, after dropping the last unrecognized optional parameter, all of the remaining unrecognized parameters still cannot be passed, the last one received (within the ones remaining) in the list is dropped. This procedure is repeated until all of the remaining unrecognized optional parameters are passed.
- The discarding of unrecognized optional parameters does not affect normal call processing (the call proceeds). If any parameter needs to be dropped, the parameter name, the length indicator of the parameter, and the parameter are all dropped simultaneously; a parameter is never altered to accommodate a fixed size limit.
- If the receiving exchange is the destination exchange of the message, then the unrecognized optional parameters are discarded without further processing. However, the discarding of this information does not affect normal call processing (the call proceeds).

5.3.4.2.2 Interaction with Q.931 Information Transport

See "Interaction with Unrecognized Optional Parameters," Section 5.4.1.2.3 for the relationship between discarding unrecognized optional parameters, UUI and ATP.

5.3.4.3 Unrecognized Parameter Values

Some unrecognized parameter values can be interpreted in a reasonable manner and default handling procedures are used at either the originating or terminating end office. If an end office, on receipt of unrecognized parameter values, needs to interwork with other signaling systems, the default interpretations of those parameter values are used to generate the corresponding signaling information in the other signaling system.

A tandem switch does not treat the unrecognized values based on the default handling procedure. Those unrecognized values are passed to the preceding/succeeding exchange as they have been received unless the selection of the outgoing circuit requires a specific field value (for example, COT required at this circuit).

Some of the unrecognized parameter values, if received by an exchange, cannot be interpreted in a reasonable way and are either given final handling treatment at the receiving switch or passed unchanged to the final destination at which point the information and the message in which the unrecognized information was received may be discarded.

5.3.5 Excessive ISDN Call Delay Notification

Excessive ISDN call setup delay handling procedures extend the basic rate interface (BRI) implementation for certain call setup error conditions for intraswitch ISDN calls to interswitch operation. This section covers procedures at tandem and originating exchanges for non-ISDN originations. See "ISDN User-Network Interface," Section 9 for originating ISDN procedures.

5.3.5.1 Call Progress Message Handling

This feature introduced the use of the Call Progress Message (CPG). See "Completion Of Transmission Path," Section 5.3.6 for transmission path completion procedures for the CPG.

5.3.5.1.1 OEO Call Progress Message Actions

Tables 5.3-5, 5.3-6, and 5.3-7 summarize the switch actions with respect to CPG messages over an ISUP trunk

at an OEO switch.

Table 5.3-5 OEO Backward CPG Received (With Cut-Through Indication)

CPG RECEIVED	ACTION
TRUNK IDLE	send RSC
BEFORE COT COMPLETE & BEFORE EXM	send RSC
BEFORE COT COMPLETE & AFTER EXM	send RSC
BEFORE EXM	cut-through, map
AFTER COT & BEFORE ACM	cut-through
AFTER ACM & BEFORE ANM	cut-through, map, process
AFTER ANM & BEFORE REL	do not map, process for Business Group info
AFTER REL BEFORE IDLE	ignore

Table 5.3-6 OEO Backward CPG Received (Without Cut-Through Indication)

CPG RECEIVED	ACTION
TRUNK IDLE	send RSC
BEFORE COMPLETION of COT	send RSC
BEFORE EXM	map
AFTER COT & BEFORE ACM	ignore
AFTER ACM & BEFORE ANM	map, process
AFTER ANM & BEFORE REL	do not map, process for Business Group info
AFTER REL BEFORE IDLE	ignore

Table 5.3-7 OEO Forward CPG Sent (Cut-Through Indication Not Valid)

CPG SENT	ACTION
CENTREX NETWORK CALL TRANSFER	send (only sent in the talking state - after ANM and before REL)
OTHER	does not generate

5.3.5.1.2 Tandem Call Progress Message Actions

Tables 5.3-8, 5.3-9, and 5.3-10 summarize the switch actions with respect to CPG messages over an ISUP trunk in a ISUP-to-ISUP tandem configuration.

Table 5.3-8 Tandem Backward CPG Received (With Cut-Through Indication)

CPG RECEIVED	ACTION
TRUNK IDLE	send RSC
AFTER FIRST FORWARD MESSAGE & BEFORE IAM (for example, CRM, CRA)	send RSC
BEFORE COMPLETION of COT	send RSC
BEFORE EXM	cut-through, pass CPG
AFTER COT & BEFORE ACM	cut-through, pass CPG
AFTER ACM & BEFORE REL	cut-through, pass CPG
AFTER REL BEFORE IDLE	ignore

Table 5.3-9 Tandem Backward CPG Received (Without Cut-Through Indication)

CPG RECEIVED	ACTION
TRUNK IDLE	send RSC
AFTER FIRST FORWARD MESSAGE & BEFORE IAM (for example, CRM, CRA)	send RSC
BEFORE COMPLETION of COT	send RSC
BEFORE EXM sent backward	pass
AFTER COT & BEFORE ACM	pass
AFTER ACM & BEFORE ANM	pass
AFTER ANM & BEFORE REL	pass
AFTER REL BEFORE IDLE	ignore

Table 5.3-10 Tandem Forward CPG Received (Cut-Through Indication Not Valid)

CPG RECEIVED	ACTION
TRUNK IDLE	send RSC

BEFORE COMPLETION of COT	send RSC
DURING COT FAIL PROCESSING	send RSC
BEFORE EXM sent backward	send RSC
AFTER COT & BEFORE ACM	send RSC
AFTER ACM & BEFORE ANM	ignore
AFTER ANM & BEFORE REL	pass
AFTER REL BEFORE IDLE	ignore

5.3.5.1.3 TEO Call Progress Message Actions

Tables 5.3-11 , 5.3-12 , and 5.3-13 summarize the switch actions with respect to CPG messages over an ISUP trunk in a terminating end office (TEO).

Table 5.3-11 TEO Backward CPG Sent (With Cut-Through Indication)

CPG SENT	ACTION
NO KNOWN SERVICES REQUIRE THIS	does not generate with cut-through indication

Table 5.3-12 TEO Backward CPG Generated (Without Cut-Through Indication)

CPG GENERATED	ACTION
CALL FORWARD VARIABLE	does not generate CPG with call forwarding indication
CALL FORWARD DON'T ANSWER	does not generate CPG with call forwarding indication
CENTREX NETWORK CALL TRANSFER	send (only sent in the talking state - after ANM and before REL)
OTHER	ignore

Table 5.3-13 TEO Forward CPG Received (Cut-Through Indication not Valid)

CPG RECEIVED	ACTION
TRUNK IDLE	send RSC
BEFORE COMPLETION of COT	send RSC
AFTER COT & BEFORE ACM	send RSC
AFTER ACM & BEFORE ANM	do not map, process for Business Group info
AFTER ANM & BEFORE REL	do not map, process for Business Group info
AFTER REL BEFORE IDLE	ignore

5.3.5.2 Procedures at a Tandem

If an ACM/ANM/CPG is received at a tandem switch and the incoming circuit is signaling system 7 (SS7) supported, the exchange formulates and sends an ACM/ANM/CPG for the incoming circuit. The parameters included in this ACM/ANM/CPG and their coding are the same as in the received ACM/ANM/CPG except for the ISUP protocol control indicator fields in the BCI parameter. These bits are coded to reflect any changes resulting from characteristics of the outgoing connection. If an OBCI parameter is received in an ACM/CPG/ANM for the outgoing circuit, the parameter is included in the ACM/CPG/ANM sent for the incoming circuit coded "as is."

When a tandem exchange receives an address complete message (ACM) with the BCI called party status field coded "excessive delay at terminating ISDN interface," an ACM is returned to the preceding exchange with the delay notification coded in the BCI parameter. See "Data Administration (Translation, Recent Change, and Verify)," Section 5.5 for details on how the ACM may be transformed into a CPG message. If the cause indicator parameter is received in the ACM, it is included in the outgoing ACM.

If a tandem exchange receives a call progress message (CPG), the message is transmitted to the preceding exchange. The CPG is passed if received on specifications shown in Tables 5.3-5 , 5.3-6 , 5.3-7 , 5.3-8 , 5.3-9 , and 5.3-10 .

Multiple CPG messages may be received at a tandem exchange for a given call. The event information parameter is transmitted to the preceding exchange with the coding unchanged. If a BCI is received, it is transmitted unchanged except that the protocol control indicator fields is updated appropriately, as noted earlier. If the cause indicator parameter is received in the CPG, it is included in the outgoing CPG. All other received optional

parameters are sent to the preceding exchange with coding unchanged.

5.3.5.3 Procedures at the Originating End Office

5.3.5.3.1 Receiving the ACM at the Originating EO

If the BCI's called party's status field is coded "excessive delay at terminating ISDN interface" it is treated as if it were coded "subscriber free." The exchange waits for an on-hook indication from the calling party or an ANM or REL message for the outgoing circuit.

5.3.5.3.2 Receiving the ANM at the Originating EO

The protocol control indicator bits of the BCI parameter, if present, are used to correct the settings of those received previously. If the BCI called party's status field is coded "excessive delay at terminating ISDN interface," it is ignored.

5.3.5.3.3 Receiving the CPG at the Originating EO

If a CPG is received at the originating end office and the originating access is non-ISDN, the protocol control indicator bits of the BCI parameter, if present, are used to correct the settings of those received previously. If the BCI's called party's status field is coded "excessive delay at terminating ISDN interface," it is ignored. If a CPG is received at the originating exchange and the CPG contains an OBCI parameter with user-network interaction indication or a BCI parameter with interworking indication, the transmission path may need to be completed (refer to "Completion Of Transmission Path," Section 5.3.6 for details). There are no further requirements for the contents of this message, so any other parameters are discarded unless otherwise specified in feature requirements. The exchange waits for an on-hook indication from the calling party, an ANM, or REL message for the outgoing circuit, or an ACM message for the outgoing circuit if a previous ACM has not been received.

5.3.6 Completion Of Transmission Path

TR-TSY-000444, Issue 1, specifies a number of changes in the procedures for completion of transmission path. These are to be principally motivated by concerns about fraudulent use of network resources. For circuit-switched data calls, the requirements call for delay of the completion of transmission path in both directions until the answer message. The CPG message may trigger cut-through for speech, 3.1 kHz audio, and data calls under certain circumstances.

The following enhancements are also available:

- The ability to cut through in both directions upon receipt of CPG with user-network interaction indication or interworking indication at the originating and tandem exchanges for all calls.
- The ability to cut through in both directions upon off-hook/access CONNECT at the terminating exchange.

5.3.6.1 Originating and Intermediate Exchanges

Regardless of the setting of the information transfer capability field of the user service information parameter, the transmission path is completed in both directions on the receipt of one of the following:

- A CPG with an "interworking encountered" coding of the backward call indicator (BCI) parameter
- A CPG with the user-network interaction indicator of the optional backward call indicator (OBCI) parameter coded "user-network interaction occurs, cut-through of bearer channel in both directions."

The timer awaiting ACM remains on if a CPG causing cut-through is received prior to the ACM.

If an ACM is received after the transmission path has been completed in both directions, owing to the receipt of a CPG with the appropriate indications, the existing procedures, with the exception of cut-through, are followed.

For a setting of the information transfer capability field of the user service information parameter of "speech" or "3.1 kHz audio," the transmission path is completed in both directions on the receipt of the ACM message, unless a previous CPG as coded previously had already triggered the cut-through.

At an interworking exchange where the incoming circuit is not SS7 supported but the outgoing circuit is, a CPG with an indication of "interworking encountered" or "user-network interaction" received before an ACM, causes cut-through with no other change in the usual message sequence for non-test calls. For test calls, a CPG received prior to an ACM with indications warranting cut-through is disregarded.

5.3.6.2 Completion of Transmission Path for Data Calls

The transmission path for a data call is not completed unless a non-ISUP trunk is encountered in the path (interworking encountered) or the originating party needs to provide additional information for the call (user interaction). Unless one of these two events occurs, the transmission path for data calls is completed when the called party answers the call. Voice traffic continues to operate as in previous software releases.

A CPG, ACM or ANM message is never sent until all continuity checks on previous circuits or the outgoing circuit for the call connection are successfully completed. If such a message is received before the completion of the continuity check, the message is treated as an unexpected message.

5.3.7 Mapping Of ACM To CPG At A Tandem Exchange

For some services, such as user network interaction or ISDN call forwarding (no reply, both ISDN and non-ISDN), an ACM may be returned from an exchange before an end-to-end signaling connection has been established for the call. When an ACM is received at an exchange that has already sent an ACM for that call, the information contained in the ACM received is relayed via the CPG to the originating end to update the end-to-end call-associated information (for example, the BCI parameter). The software release mechanism for mapping ACM to CPG, which is performed as a part of basic signaling protocol procedures independent of the particular service that caused the ACM to be returned before establishing end-to-end signaling connection, has recently been agreed to in T1S1 standards.

The following abilities are provided:

- The ability to generate a CPG upon receipt of an ACM, if the exchange has previously sent an ACM for the call.
- The ability to encode the mandatory event information parameter in the CPG based on the BCI parameter and the OBCI parameter received in the ACM.
- The ability to update the protocol control indicator of the BCI parameter and include all parameters received in the ACM in the CPG generated.

5.3.7.1 Action at a Tandem Exchange

The receipt of an ACM at the intermediate exchange, which has previously sent an ACM and is waiting for an ACM on the outgoing circuit for this call, causes the exchange to do the following:

- Cancel the awaiting address complete timer.
- Send a CPG to the preceding exchange containing all of the parameters in the ACM received. The mandatory event information parameter in the CPG, indicating the reason for sending the CPG, is set based on the called

party status field in the BCI parameter received in the ACM as follows:

- The called party status field is set to "subscriber free."

The event value in the event information parameter indicates "ALERTing."

- The called party status field is set to "delay at the terminating interface."

The event value in the event information parameter indicates "Progress."

- The called party status field is set to "no indication."

If the BCI parameter of the received ACM indicates that interworking has occurred at a succeeding exchange, the event information parameter contains an event value of "Progress."

If the BCI parameter indicates that no interworking has occurred at a succeeding exchange, and if the ACM contains the OBCI with the indication that inband information is available, the event value in the event information parameter is set to "inband information now available."

Otherwise, the event information parameter is set to "Progress."

- The called party status field is set to "connect when free."

The event value in the event information parameter indicates "Progress."

The BCI parameter received in the ACM is coded unchanged in the CPG generated, except that the protocol control information field is updated.

All other optional parameters received in the ACM are coded unchanged in the transmitted CPG.

The transmission path at the exchange mapping ACM to CPG may need to be completed upon receipt of ACM for the outgoing circuit. Unless a particular feature specifies otherwise, the procedures in "Completion Of Transmission Path," Section 5.3.6 are followed.

The receipt of an ACM at the exchange, which has previously sent an ACM and is in the talking state for the call, causes the exchange to discard the ACM.

5.3.8 Coding of 3.1 kHz Audio Bearer Capability

5.3.8.1 Bearer Capability Determination

At originating or intermediate LEC switches, an incoming call using an inband signaling voice trunk is identified as using a bearer capability of "3.1 kHz audio" for error treatment purposes. This includes multifrequency (MF), dial pulse (DP), and touch-tone (TT) trunks.

At an originating LEC switch, a non-ISDN access call is identified as using a bearer capability of "3.1 kHz audio" for error treatment purposes. This means that all analog line originations have a bearer capability of "3.1 kHz audio."

At an originating switch, an incoming ISDN access (PRI and BRI) call is identified by the bearer capability received in the bearer capability IE of the Q.931 SETUP message for error treatment purposes.

NOTE: There is no distinction between an incoming PRI at an LEC switch and an incoming PRI at a toll switch. Both calls are assigned the bearer capability received in the Q.931 SETUP message.

At an intermediate switch, incoming calls received on an ISUP trunk are identified by the bearer capability received

in the Information Transfer Capability (ITC) field in the User Service Information (USI) parameter of the Initial Address Message (IAM) for routing and error treatment purposes.

5.3.8.2 Coding of the ITC Field in the Outgoing IAM

The per-trunk group parameter, RCD 3PT1 ITC, on Recent Change/Verify View 5.1 is used to recode the information transfer capability (ITC) assigned to a call. This indicator is only checked for calls that have an information transfer capability of "3.1 kHz audio." A local tandem assigns an ITC of "3.1 kHz audio" to a call it receives over an inband signaling speech trunk. Before routing this call out of the office over an ISUP trunk, the RCD 3PT1 ITC indicator is checked to determine the setting for the information transfer capability in the outgoing ISUP IAM. This indicator is also checked at all originating end offices for non-ISDN originated calls that are about to be routed out of the end office via an ISUP trunk.

If the value of the trunk group parameter is set to "speech," the ITC in the outgoing IAM is recoded to "speech." If the value of the per-trunk group indicator is set to "3.1 kHz audio," the ITC in the outgoing IAM remains "3.1 kHz audio." If the per-trunk group field, RCD 3PT1 ITC, is left blank, the setting of the ITC in the outgoing IAM is determined by the global office parameter, RCD 3PT1 ITC, on Recent Change/Verify View 8.15.

The global office parameter, RCD 3PT1 ITC, is only referenced when the per-trunk group indicator, RCD 3PT1 ITC, is left blank. If the per-trunk group indicator is blank and the global office parameter is set to "speech," then the ITC in the outgoing IAM is recoded to "speech." If the per-trunk group indicator is blank and the global office parameter is set to "3.1 kHz audio," the ITC in the outgoing IAM is sent as "3.1 kHz audio" without being recoded.

NOTE: Although the per-trunk group indicator and the global office parameter are checked in both local and toll offices, there are recent change/verify rules which prevent the toll office settings from being updated. The toll office settings must always be set to pass the ITC through as it was received.

5.3.9 Routing Based on Bearer Capability

Bellcore TR-TSY-000448, *ISDN Routing and Digit Analysis* requires that "speech" and "3.1 kHz audio" calls be routed differently. The Routing Based On Bearer Capability feature provides flexible routing for "speech" and "3.1 kHz audio" calls. "3.1 kHz audio" calls equate roughly to voiceband data (facsimile, modems, etc.) where it is important to maintain the absolute integrity of the bit stream. A call with the bearer capability of "3.1 kHz audio" is routed out of a switch over the following types of trunks:

- any voice trunks with no "speech" treatment
- ISUP 56K data trunks
- ISUP R64K data trunks
- ISUP 64C data trunks.

"Speech" calls are allowed to be routed out of a switch over the speech facilities [that is, trunks which have speech treatments (such as, Time Assignment Speech Interpolation (TASI) and Low Bit Rate Voice (LBRV) encoding)].

Craft personnel can provision a trunk group selection list for "3.1 kHz audio" calls. However, trunk groups in the 3.1 kHz audio list should not have the following "speech" characteristics:

- Echo controlled voice transport (either 2- or 4-wire)
- Signal compression hardware
- time assignment speech interpolation (TASI) mechanisms

- Low bit rate voice (LBRV) mechanisms.

The previous restrictions are not enforced by the switch to allow maximum flexibility.

Switch personnel can provision a separate trunk group selection list for "speech" calls. The trunk group selection list for "speech" calls should generally contain "speech" capable trunks. However, at the option of switch administration, "3.1 kHz audio" capable trunks may be included in the trunk group selection list for "speech" calls (this is known as upgrade routing and is described in more detail later in this section).

The concept of two trunk group selection lists, one for voice and one for 3.1 kHz, does not apply to any feature that bypasses the screening mechanism in the routing process [such as, Automatic Route Selection (ARS), Private Facility Access (PFA), etc.]. This means that a feature call with bearer capability of "speech" should be routed to the trunk groups referenced in the feature list and should not be diverted to trunks in a "speech" trunk group selection list.

Calls outgoing on an ISUP trunk which are marked with a bearer capability of "3.1 kHz audio" and are being routed out over a trunk group marked "speech" will be processed with a warning to switch personnel.

5.3.9.1 Upgrade Routing

When the call volume is greater than the capacity of the primary trunk group to a particular destination, secondary route indexes are used to overflow to other trunk groups to that destination. If the primary trunk is "speech," then the secondary routes could be the same as routes for "3.1 kHz audio" (that is, the existing voice routes). In other words, a "speech" bearer capability call can be routed over a greater capability route, one that does not have "speech" treatments. The secondary routes could be additional "speech" trunk groups and may be set up to never overflow to the "3.1 kHz audio" routes.

Since the default bearer capability for incoming calls over MF "non-data" trunks or calls originating from non-ISDN access lines will be "3.1 kHz audio," and since most ISDN calls are likely to use a bearer capability of "3.1 kHz audio," these calls will use the current voice routing scheme. This implementation is done for efficiency and to minimize the impact on offices that do not have "speech" trunk groups.

5.4 FEATURE APPLICATIONS

5.4.1 Q.931/ISUP Information Transport

5.4.1.1 User-to-User Information

If both calling and called parties are ISDN subscribers, the parties may transfer user-to-user information through the signaling network during the call setup and clearing phases.

The ISUP messages used to carry the user-to-user information are:

- Initial Address Message (IAM)
- Address Complete Message (ACM)
- Answer Message (ANM)
- Release Message (REL).

Each of these messages has a user-to-user information parameter that is used to carry this information. Interworking between the Q.931 and ISUP that is required to provide user-to-user information is covered in "ISDN User-Network Interface," Section 9 of this document.

5.4.1.2 Separate Capabilities

The feature has been broken into two separate capabilities, "User-to-User Signaling" and "Q.931 Information Element Transport." This allows the transfer of 129 bytes Q.931 information elements in the access transport parameter and a total of 131 bytes *user-to-user information*, including the parameter name code and length indicator.

The Facility Reject message is not used backwards notification when UUI/ATP are discarded. For integrated services digital network (ISDN) backward compatibility, the use of the facility reject message continues to be supported when ATP parameter, UUI parameter information, or both ATP and UUI parameter information is lost due to signaling interworking, internetwork screening, etc.

NOTE: Loss of "all user data" means that either access transport parameter alone or both access transport parameter and *user-to-user information* was received, but neither access transport parameter nor *user-to-user information* is included in the outgoing message.

However, facility reject is not supported across network boundaries.

5.4.1.2.1 Q.931 Information Element Transport (ATP)

The Access Transport Parameter (ATP) is an envelope provided in ISDN for the transport of Q.931 information elements transparently through the network.

Bellcore, ANS[®], and T1S1 standards have specified specific information elements for transport in the access transport parameter. In addition, the *Message Associated with User-to-User Information* feature allowed the transporting of some additional IEs in the access transport parameter.

The following enhancements have been made:

- The size of the ATP is increased to 129 octets (not including the parameter identifier and the length indicator).
- The ATP and the UUI parameter is decoupled and no combined length check is performed.

- ATP is given a higher priority than the UUI parameter when information is discarded.
- No explicit notification via the Facility Reject message is provided if the information is discarded.

5.4.1.2.1.1 Normal Operations

The messages that are allowed to carry ATP are the following:

- Initial Address Message (IAM)
- Address Complete Message (ACM)
- Answer Message (ANM)
- Call Progress Message (CPG)
- Release Message (REL).

The ATP is capable of transporting 129 octets of user data (not including the parameter name code and the length indicator). No combined length check with the User-to-User parameter is performed.

If the total ISUP message length exceeds 272 octets, the ATP may be dropped (refer to "Interaction with Unrecognized Optional Parameters," Section 5.4.1.2.3 for details).

5.4.1.2.1.2 Originating End Office

- Forward Messages

The ATP can be included in IAM or the first clearing message. The originating switch checks the size of ATP. If the size of ATP exceeds 129 octets (not including the parameter name code and the length indicator of the ATP), the ATP is discarded without affecting the normal call processing. Otherwise, the switch passes the ATP.

- Backward Messages

The ATP can be received in an ACM, ANM, CPG, or REL message. If the length of ATP exceeds 129 octets, the ATP is discarded.

5.4.1.2.1.3 Tandem Office

The tandem switch may check the length of the ATP. If the length of ATP in the received message exceeds 129 octets (not including the 2 octets header), the ATP may be discarded. Otherwise, the ATP is always passed (unless dropped due to screening as specified in "5E7 and Later Software Releases," Section 10.3.3.2.3).

The tandem switch does not examine the content of the ATP. All the Q.931 IEs received in the ATP remain in the ATP and are passed to the succeeding office.

The ATP is decoupled from the UUI parameter. No combined length check is performed at a tandem switch. The ATP is given a higher priority than the UUI parameter when information is discarded.

A tandem switch does not generate the Facility Reject message if it discards the ATP for any reason. A tandem switch discards the Facility Reject message if it receives one.

5.4.1.2.1.4 Terminating End Office

For a terminating office, the following messages apply:

- Forward Messages

The ATP can be present in an IAM or REL message. The terminating switch checks the length of the ATP. If the length of ATP in the received message exceeds 129 octets (not including the 2 octets header), the ATP is discarded.

The terminating exchange unpacks the information and passes it to the Q.931 process for delivery to the CPE.

- Backward Messages

The access transport parameter can be present in an ACM, ANM, CPG, or REL message. The terminating switch checks the length of the access transport parameter. If the total length of the Q.931 information elements in the access transport parameter in the received message exceeds 129 octets (not including the 2 octets header), the access transport parameter is discarded.

5.4.1.2.1.5 Exceptional Operations

Receipt of an ATP parameter in any SS7 message for a non-ISDN originated call is unexpected, and these parameters are discarded. No explicit forward notification (Facility Reject message) is sent to the called party upon discarding an ATP or UII parameter.

If an ATP is detected within any other messages not mentioned previously, the ATP is discarded without affecting the normal call proceeding. No Facility Reject message is generated if the information is discarded for any reason. Tandem switches do not relay the Facility Reject message.

5.4.1.2.2 User-to-User Information Signaling (UII)

User-to-User Information Signaling allows ISDN customers to exchange user data transparently through the network during call setup and call clearing. The user-to-user information may be discarded if switch resources become constrained.

The following enhancements have been made:

- The size of the User-to-User Information (UII) parameter is increased to 129 octets (not including the parameter identifier and the length indicator).
- The ATP and the UII parameter is decoupled and no combined length check is performed.
- ATP is given a higher priority than the UII parameter when information is discarded.
- No explicit notification via the Facility Reject message is provided if the information is discarded.

5.4.1.2.2.1 Normal Operations

The messages that are allowed to carry UII are the following:

- Initial Address Message (IAM)
- Address Complete Message (ACM)
- Answer Message (ANM)

- Call Progress Message (CPG)
- Release Message (REL).

NOTE: Bellcore TR-845 requires that no *user-to-user information* is included in SS7 ACM or SS7 CPG with event indicator coded "ALERTING"/ "PROGRESS."

The UUI parameter should be capable of transporting 129 octets of user provided information (not including the parameter name code and the length indicator). No combined length check with the Access Transport Parameter will be performed.

If the total message length exceeds 272 octets, the UUI may be dropped (refer to "Interaction with Unrecognized Optional Parameters," Section 5.4.1.2.3 for details).

5.4.1.2.2.2 Originating End Office

For an originating office, the following messages apply:

- Forward Messages

The UUI can be included in IAM or REL messages. The originating switch checks the size of UUI. If the size of UUI exceeds 129 octets (not including the parameter name code and the length indicator of the UUI), the UUI is discarded without affecting the normal call processing. Otherwise, the switch passes the UUI.

- Backward Messages

UUI can be received in an ACM, ANM, CPG, or REL message. If the length of UUI exceeds 129 octets, the UUI is discarded.

5.4.1.2.2.3 Tandem Office

The tandem switch may check the length of the UUI. If the length of UUI in the received message exceeds 129 octets (not including the 2 octets header), the UUI may be discarded. Otherwise, the UUI is always passed (unless dropped due to screening as specified in "5E7 and Later Software Releases," Section 10.3.3.2.3).

The UUI is decoupled from the ATP parameter. No combined length check is performed at a tandem switch. UUI is given a lower priority than the ATP parameter when information is discarded.

A tandem switch does not generate the Facility Reject message if it discards the UUI parameter for any reason. A tandem switch discards the Facility Reject message if it receives one.

5.4.1.2.2.4 Terminating End Office

For a terminating office, the following messages apply:

- Forward Messages

The UUI can be present in an IAM or REL message. The terminating switch checks the length of the UUI. If the length of UUI in the received message exceeds 129 octets (not including the 2 octets header), the UUI is discarded.

The terminating exchange unpacks the information and passes it to the Q.931 process for delivery to the CPE.

- Backward Messages

The UUI parameter can be present in an ACM, ANM, CPG, or REL message. The terminating switch checks the length of the UUI. If the total length of the UUI parameter in the received message exceeds 129 octets (not including the 2 octets header), the UUI is discarded.

5.4.1.2.2.5 Exceptional Operations

Receipt of a UUI parameter in any SS7 message for a non-ISDN originated call is unexpected, and these parameters are discarded. No explicit forward notification (Facility Reject message) is sent to the called party upon discarding an ATP or UUI parameter.

If UUI is detected within any other messages not mentioned previously, the UUI is discarded without affecting the normal call proceeding. No Facility Reject message is generated if the information is discarded for any reason. Tandem switches do not relay the Facility Reject message.

5.4.1.2.3 Interaction with Unrecognized Optional Parameters

If the total size of an ISUP message, including UUI, ATP, and unrecognized optional parameters formulated for sending to the succeeding/preceding exchange, is greater than 272 bytes (including the 7 bytes routing label), the UUI parameter is discarded without affecting normal call processing (the call proceeds as if no UUI has been discarded) and no notification is sent back to the sender of the UUI. If after discarding the UUI parameter, the message is still greater than 272 bytes, the ATP is dropped without affecting normal call processing (the call proceeds as if no ATP has been discarded) and no notification is returned to the sender of the ATP. If after dropping the ATP, the message size is still greater than 272 bytes, the unrecognized optional parameters are dropped until the message size drops to 272 bytes.

NOTE: Since the parameters are not altered, the resulting actual message size may be less than 272 bytes.

5.4.2 Customer Account Services Enhancements

Refer to "Customer Account Services Enhancements," Section 11.13.1 for detailed specifications of OSPS use of ISUP.

5.4.3 Generic Address Parameter (GAP)

The generic address parameter (GAP) is transported in the IAM. The GAP is only passed in a tandem office if such a parameter is received on an ISUP-to-ISUP connection.

The GAP parameter is understood on input in an IAM message and can be sent out in an IAM message, but it is not interworked from non-CCS signaling at an OEO switch. It is also not interworked to non-CCS signaling at a TEO switch.

GAP may be generated by an OSPS office to carry a third party number value.

5.4.3.1 Tandem Office

On receipt of one or more GAPs, the tandem office does the following:

If the received GAP has a type of address of "User provided, failed screening" or "User provided, not screened," it is passed in the GAP parameter. A received GAP with any other type of address is passed as an unrecognized parameter. Note that only the first instance of a GAP parameter of the user provided type is passed in the GAP parameter, any other subsequent GAPs of the user provided type are passed as unrecognized.

Any per-IEC CPN subscription options will also control the sending of the GAP parameter; this applies only to the

recognized GAP parameter. Unrecognized parameters, including GAPs of type other than User provided, are passed unchanged.

5.4.4 Delivery Of Calling Party Number and Charge Number

The optional calling party number parameter and the charge number parameter may be included in the IAM. The transit exchange passes these parameters through unchanged within a network.

5.4.4.1 Address Digits

The calling party number parameter carries the address digits of the specific station set originating the call. This is either the user-provided station identification or network-provided directory number. The calling party address information always includes the ten NPA-NXX-XXXX digits in the address information field, if available. If the entire ten digits of the calling party address are not available, the end office includes the six NPA-NXX digits, when available. Otherwise, it includes the three NPA digits.

The charge number information always includes the ten NPA-NXX-XXXX digits in the address signals, if available. If these are not available, the three NPA digits are included. If no automatic number identification digits are available, the parameter is still included; however, the address digits are omitted.

5.4.4.2 Privacy Indicators

The calling party parameter contains privacy indicators which determine whether the calling party information may be displayed upon termination. Customers presubscribe to a privacy indication for their network-stored calling party number. However, when the customer provides the calling party number station identification, the presubscription is overridden by the calling party number information. If the calling party number is user-provided through the ISDN User-Network Interface (Q.931) calling party number information element, the procedures used are in "ISDN User-Network Interface," Section 9.

For specifics on code sets for each field in this parameter, refer to Bellcore's TR-NWT-000246.

Privacy bits in the CHG parameter are always generated as 00. Bellcore ISUP does not recognize privacy bits in the CHG parameter.

5.4.5 Generic Name Parameter

The generic name (GN) parameter is introduced via the Analog Calling Name Delivery - Phase 2 special feature (99-5E-0834). This feature delivers the name associated with the calling line to called analog subscribers with special customer premises equipment (CPE). It also provides for invocation of privacy features by the originator to specify the originator's per-call preference for having his or her name publicly displayed to the called party.

The 5E13 software update feature Originating Switch Calling Name (99-5E-4684) modifies Analog Calling Name Delivery to allow a 5ESS[®]-2000 switch to send a calling party name (stored on the switch or obtained from a TCAP query to the Calling Name database) on an outgoing interswitch SS7 call and to receive a calling party name on an incoming SS7 call.

For further information on the GN parameter, Analog Calling Name Delivery - Phase 2, and the Originating Switch Calling Name feature, refer to 235-190-130, *Local Area Signaling Services (LASS)* feature document.

For further information on Originating Switch Calling Name feature interactions with the Advanced Intelligent Network (AIN) and Terminating Attempt Trigger (TAT), refer to 235-190-126, *Advanced Services Platform — Release 0.1B*.

5.4.5.1 Originating Office

An originating office includes the GN parameter in the IAM message. This parameter includes information showing that the caller dials a name privacy code: Name Privacy (NAP), Name/Number Privacy (NNP), or Name/Number Display Allowed (NNDA). The length of the GN parameter is variable, from 3 to 18 octets: 1 octet for parameter name; 1 octet for parameter length; 1 octet containing the type of name, availability, and presentation indicator; and up to 15 octets (15 characters) of calling name information. When no name characters are included, the length of the parameter generated is 3 octets.

The availability field in the GN parameter is set to "Name Available" only when a 10-digit calling party number (CPN) parameter is included in the outgoing IAM. Otherwise, the availability field is set to "Name Not Available." The type of name field of the GN is always set to "Calling Name."

5.4.5.2 Intermediate Office

Intermediate office functionality is not secured. The GN parameter is passed through an intermediate switch with some Originating Switch Calling Name feature functionality:

- a GN parameter with name text longer than 15 characters is truncated to only 15 characters, and
- a cross check occurs between the name text and the availability bit. If the text is null and availability is coded as "Name Available," then the availability bit is reset to "Name Not Available."

5.4.5.3 Terminating Office

If a GN parameter is received with the type of name field set to a value other than "Calling Name," the parameter is not processed with Originating Switch Calling Name feature functionality.

Even though the switch does not generate the name characters in the GN parameter, if an intermediate switch receives the name characters in the GN, the information is transparently passed through the switch.

If a valid GN parameter is received at a terminating end office with the availability field set to "Name Available" and the presentation indicator allows display of the calling name, the calling name is delivered to the called party (provided the called party subscribes to calling name display). If the GN parameter is received without a calling name, or no GN parameter is received, and if the switch is provisioned to do calling name (CNAM) TCAP queries, then the terminating switch attempts to retrieve the calling name through a CNAM TCAP query (provided the called party subscribes to calling name display).

5.4.6 Forced Calling Number Privacy on CCS Trunks

5.4.6.1 Description

The "Forced Calling Number Privacy on CCS Trunks" feature (99-5E-1627) prevents the calling party number (CPN) leaving a 5ESS®-2000 switch over Common Channel Signaling 7 (CCS7) trunks from being displayed at a far-end (terminating) office. Subscribers at the far-end office receive a display of "PRIVATE NUMBER" on their display handsets.

This feature is secured (SFID 27) and requires that necessary arrangements be made between the service provider and Lucent Technologies. These arrangements include paying a right-to-use (RTU) fee before Lucent Technologies provides enabling information.

5.4.6.2 Cross References

- Feature number: 99-5E-1627
- Bellcore specifications: None

5.4.6.3 Background

Not applicable.

5.4.6.4 Availability

The "Forced Calling Number Privacy on CCS Trunks" feature was implemented in the 5E9(1) software release.

5.4.6.5 Feature Environment

This feature is provided on a per-office basis and is active only on CCS7 trunks.

5.4.6.6 Feature Operation

The "Forced Number Privacy on CCS Trunks" feature sets the CCS7 initial address message's (IAM) Calling Party Presentation Restricted Indicator to "restricted" for all CCS7 calls leaving the office. This prevents the far-end office from displaying the originator's directory number. Those lines at the far-end office provisioned with the Calling Number Display feature will have the incoming caller's directory number blocked from appearing on their display handsets.

5.4.6.7 User Operation

5.4.6.7.1 For Subscribers

No subscriber action is associated with this feature.

5.4.6.7.2 For Switch Personnel

No switch personnel action is associated with this feature.

5.4.6.8 Engineering

5.4.6.8.1 Hardware Resources

This feature requires no new hardware.

5.4.6.8.2 Software Resources

This feature requires no new software resources.

5.4.6.8.3 Transition Considerations

There are no transition considerations associated with this feature.

5.4.6.9 Interactions and Limitations

The "Forced Calling Number Privacy on CCS Trunks" feature has no effect on calls made within the same switch.

Calls forwarded out of the office over CCS7 trunks with the "Forced Calling Number Privacy on CCS Trunks" feature installed will always have the CPN of the originating caller forced as "private." If the originating call is forwarded by a second party (either within the originating office or from the office to which the call terminated), the second party's CPN has the default privacy associated with the second party's line and is not affected by this feature.

Although the CPN of the originating caller is always marked as "private," the name of the originating caller may sometimes be displayed if the Calling Name Display (CNAM) feature is active at the terminating office. With CNAM active, the calling name/number display of the called party displays the calling name and/or number (or is marked "private") from information in the external Name Number Data Base (NNDB) stored at the service control point (SCP).

Normally, however, the originating caller dials one of the following access codes to control the information displayed on the called party's handset:

- Name Privacy (NAP)
- Name/Number Privacy (NNP)
- Name/Number Display Allowed (NNDA)

If the originating caller does not dial an access code and the terminating office has the CNAM feature enabled and RC view 8.31 (OPTIONED FEATURES), field **FEATURE ID** set to **541** and field **ACTIVE** set to **Y** [to prevent a query of the external NNDB stored at the SCP], the name privacy status is forced to "private" and the calling party's NAME is not displayed.

If the originating caller does not dial an access code and the terminating office has the CNAM feature enabled and RC view 8.31, field **FEATURE ID** set to **541** and field **ACTIVE** set to **N**, a query of the external NNDB stored at the SCP is allowed and the display of the calling party's NAME is provided (or marked "private") based on information in the NNDB. It is important to note that the later phases (2 and 2.1) of the CNAM feature are likely to have RC view 8.31, field **ACTIVE** set to the default value of **N**.

5.4.6.10 Incompatibilities

This feature has no incompatibilities.

5.4.6.11 Dependencies

This feature has no dependencies.

5.4.6.12 Isolation Constraints

This feature has no isolation constraints.

5.4.6.13 Feature Implementation

5.4.6.13.1 Office Data Administration (ODA) Provisioning

The following table provides a cross-reference between ODA forms and the associated Recent Change views. The ODA forms must reflect the same information shown in section 5.4.6.13.2.

ODA FORM NAME	OFFICE RECORD	ASSOC RC/V VIEW
sfsys	5317-1	8.22

NOTE: Refer to 235-080-100, *Translation Guide* for details on translations forms.

5.4.6.13.2 Recent Change Provisioning

The service provider enables the "Forced Calling Number Privacy on CCS Trunks" feature by populating Recent Change view 8.22 as follows:

FIELD	VALUES
FEATURE ID	27
MODULE	OFC
PASSWD	(Obtain from Lucent Technologies SFID Administrator)
ACTIVE	Y

NOTE: Allowed values for all Recent Change views may be found in 235-118-2xx, *Recent Change Reference*.

5.4.6.13.3 Customer Premises Equipment (CPE)

No special CPE is required for this feature.

5.4.6.14 Maintenance Considerations

This feature requires no maintenance considerations.

5.4.6.15 Administration

5.4.6.15.1 Measurements

This feature requires no new measurements.

5.4.6.15.2 Billing

This feature does not affect billing.

5.5 DATA ADMINISTRATION (TRANSLATION, RECENT CHANGE AND VERIFY)

The switch provides the capability to enter the following translation data by recent change messages and bulk office data loading processes. The data can be retrieved by verify messages or office record category. See 235-080-100, *Translations Guide (TG-5)* for details of data records entries.

5.5.1 Circuit Group Characteristics

ISUP is provisioned on a trunk group basis. The smallest unit allowed for ISUP in a switch office is a trunk group.

Circuit group characteristics relating to ISUP circuit groups include continuity-checking procedures, double seizing control, and carrier group alarm protection.

- The continuity check for ISUP may be performed:
 - Any time for all circuits in a group
 - On a statistical basis
 - Not as a function of the transmission characteristic of the circuit groups.

Office data, on a per-circuit group basis, is provided to specify which continuity-check procedure is applicable.

- When double seizing occurs on an ISUP circuit, the switching exchange that is specified as the control exchange continues the initial call for that circuit. The non-control exchange backs down and retries on another circuit. The control of the circuit is either based on odd/even method or all/none method. When the odd/even method of circuit control is used, the exchange having the highest point code controls the even circuits, and the other exchange controls the odd ones. In the all/none method of circuit control, an exchange controls all of the circuits in a circuit group and the other controls none of the circuits in the same group.
- A distinction between whether a particular facility group is protected by hardware or software carrier group alarms is provided as part of the office data on a facility group basis. This allows the exchange to follow separate specified procedures as a function of the type of protection provided.

In an SS7 exchange, it is possible to designate all necessary data items including the following:

- Whether or not the circuit is a satellite circuit for coding the nature of connection indicator parameter (on a per-SS7 circuit basis).
- Whether the circuit requires the use of an outgoing "full echo suppressor," a "half echo suppressor," (echo canceler) or nothing (on a per-SS7 circuit basis).
- The procedure for providing inband tones and announcements with the choice of one or the other, along with corresponding timer or number of repetitions (on a per-exchange basis).
- Whether presentation of the calling party number and billing number (automatic number identification) is restricted or allowed (on a per-originating line basis). The calling party number is included in the IAM based on bilateral agreement between interexchange and exchange carriers. It is available on all intra-LATA calls.

5.5.2 Translations

The translation subsystem is responsible for the translation data structures needed to store SS7 related information. Routines to retrieve the information from the data structures are also provided by the subsystem.

Translations are used to associate unique point codes and circuit identification codes.

The trunk maintenance subsystem must translate a hardware carrier group or software carrier group to a list of circuit identification codes contained in that group.

5.5.3 SS7 Recent Change Implementation

Table 5.5-1 shows the ISUP related Recent Change fields. Refer to the appropriate sections of 235-080-100, *Translation Guide (TG-5)*, for a detailed description of each field and possible values that can be used to populate each field.

Table 5.5-1 Recent Change Views

VIEW NUMBER AND FIELD NAME	DESCRIPTION
8.15 CNI EQUIP	Enter Y if CNI is equipped.
8.15 DLN EQUIP	Enter Y if DLN is equipped.
8.15 DS SPEED	For AT&T Network, Low Speed=48 For AT&T Network, Low/Hi=560 For LEC Set to 48
8.15 SSP	Enter Y if SSP 800 feature is used in this office.
8.15 LATA	Identification if default LATA for this office.
8.15 ADDR COMP	Wait for Address Complete Timer
8.15 ANSWER	Wait for Answer Timer
8.15 RLS GRD	Short timer waiting for RLC after sending REL
8.15 TRD	Timed Release Disconnect Timer
8.15 TRK QRY AU	Controls rate of automatic Trunk Query audits.
8.15 CQ START TIME	Controls circuit query start time (NULL indicates no automatic office-wide circuit query will be scheduled)
8.15 COT RETST	COT Retest Interval
8.15 RSC SHORT	Short timer waiting RLC after sending REL
8.15 RSC LONG	Long timer waiting RLC after sending REL
8.15 BLO RSND	BLO Resend Interval
8.15 UBL RSND	UBL Resend Interval
8.15 COT	Wait for COT Timer
8.15 GBLO RSND	CGB Resend Timer
8.15 GUBL RSND	CGU Resend Timer
8.15 RLS COMP	CCS release complete message timer
8.15 CRA TIMER	Wait for CRA Timer
8.15 EXM D TIMER	Exit Message Timer
8.15 BUSY ANNC	Controls Sending REL with Cause=17 or playing busy tone at the terminating office
8.15 LEC ANNC	Controls Playing Tones/Announcements in LEC Network
8.15 LEC IW ANNC	Controls playing Tone/Announcements for calls that do not use ISUP7 trunks all the way.
8.15 RCD 3PT1 ITC	Controls Recoding of 3.1 kHz Audio Information Transfer Capability in Outgoing IAM Messages.
8.15 IAM CRM PRIOR	Controls IAM and CRM message priority. Implemented in 5E13.
8.15 GRA SHORT	Controls how long to wait for GRA after sending a GRS message.
8.1 SPEECH TRK GRPS	Indicates number of trunk groups which have speech treatments applied.
8.1 CICP BLK	Block sending CICP MF-ISUP interworking
5.1 TRK QUERY	Enter Y to allow the automatic Trunk Query Interoffice audit.
5.1 TRANS TEST	Translation Verification Test
5.1 VPA RATE	Controls the proportion of calls for which the Continuity test is run.
5.1 VPA TYPE	Controls the type of Continuity test that is run.
5.1 DEST PT CODE	Destination Point Code of the Far Office
5.1 ORIG PT CODE	Origination Point Code of this Office
5.1 GLARE ACTION	Controls action taken when glare is encountered.
5.1 SS7 TYPE	BELLCORE means process ISUP7 parameters as specified by Bellcore. ATT means process ISUP7 parameters as specified by AT&T NSD.
5.1 CPN RSTRCT	Restricts Sending of the CPN Parameter
5.1 CHG RSTRCT	Restricts Sending of the CHG Parameter
5.1 CFN RSTRCT	Restricts Generation of the CFN Message
5.1 ATP IC RSTRCT	Restricts sending of the ATP parameter

5.1 UUI/IC RSTRCT	Restricts sending of the UUI parameter
5.1 NI ANNC	Controls Tone/Announcements at a Network Boundary
5.1 NI IW REL	Controls Tone/Announcements at a Network Boundary for calls that do not use ISUP7 all the way.
5.1 RCD 3PT1 ITC	Controls recoding of 3.1 kHz audio information transfer capability in outgoing IAM messages.
5.1 CONTROL TYP	Controls skip cancel for network management.
5.1 SPEECH TRMTS	Designates trunk group as capable of carrying speech calls
5.1 TRK MBGID	Dedicated MBGID
5.1 ISUP MLD	Enter Y to turn on Message Loop Detection Hop Counter) Feature
5.1 MAX HOP CNT	Number of hops (value 1-20)
5.5 CLCI TRK ID	Circuit Identification Code used to identify the trunk.
10.1 PLAY ANNC	Controls Tone/Announcements at the originating toll office.
10.2 CICIP SUBSC	Carrier Identification Code Parameter subscription
10.2 ANI IND	Controls sending of billing number.
10.2 CKT CODE	Circuit Code Used in the TNS parameter of the IAM message.
10.2 CPN SUBSC	Calling Party Number Subscription
10.2 CSI SUBSC	Carrier Selection Information Parameter Subscription
10.2 ATP SUBSC	Access Transport Parameter Subscription
10.2 UUI SUBSC	User-to-User Information Parameter Subscription
10.2 SPEECH ALT RI	Identifies that this ROUTE INDEX is associated with SPEECH treatment.

5.5.4 Verification

RC/V can be used to verify the data stored in the SS7 ISUP translations.

5.5.5 OP:SS7 to Obtain SS7 Code Numbers

The I/O Message to Obtain SS7 Code Numbers feature is a maintenance tool to aid maintenance personnel in resolving problems with SS7 trunks. This feature provides the ability to obtain information on SS7 trunks through the use of the OP:SS7 input message.

The OP:SS7 input message allows the customer to input specific SS7 trunk information and obtain DPC, OPC, CIC, SS7 TG number, and TG member number information which is reported in the OP:SS7 output message. It is assumed that the DPC, OPC, and CIC together uniquely identify an SS7 trunk group and trunk member.

Table 5.5-2 identifies the input and output relationships.

Table 5.5-2 OP:SS7 Message Information

Input Options	Output Information
OFFICE ^a	TG Number(s), DPC(s) and OPC(s)
DPC	TG Number(s) (5E11 and earlier) TG Number(s), DPC and OPC(s) (5E12 and later)
OPC ^a	TG Number(s), DPC(s) and OPC
OPC and DPC ^a	TG Number(s), DPC and OPC
DPC with CIC and ALL keywords (all CICs) ^b	TG Number(s), TG Member Number(s), DPC, OPC(s), and CIC(s)
DPC with CIC range ^b	TG Number(s), TG Member Number(s), DPC, OPC(s), and CIC(s)
DPC with one CIC ^b	TG Number(s), TG Member Number(s), DPC, OPC(s), and CIC(s)
OPC with CIC and ALL keywords (all CICs) ^{a b}	TG Number(s), TG Member Number(s), DPC, OPC(s), and CIC(s)
OPC with CIC range ^{a b}	TG Number(s), TG Member Number(s), DPC, OPC(s), and CIC(s)
OPC with one CIC ^{a b}	TG Number(s), TG Member Number(s), DPC, OPC(s), and CIC(s)
DPC and OPC with CIC and ALL keywords (all CICs) ^{a b}	TG Number(s), TG Member Number(s), DPC, OPC, and CIC(s)
DPC and OPC with CIC range ^{a b}	TG Number(s), TG Member Number(s), DPC, OPC, and CIC(s)
DPC and OPC with one CIC ^{a b}	TG Number(s), TG Member Number(s), DPC, OPC, and CIC
Trunk Group Number ^b	TG Number, TG Member Number(s), DPC, OPC, and CIC(s)
Trunk Group Number with Member Number range ^b	TG Number, TG Member Number(s), DPC, OPC, and CIC(s)
Trunk Group Number with one Member Number ^b	TG Number, TG Member Number, DPC, OPC and CIC

Notes:

- a. This option is available beginning in the 5E12 software release. It accommodates multiple OPC assignments in a single 5ESS®-2000 switch. See "SS7 Access on a PSU Platform," Section 12, for details.
- b. Beginning in the 5E12 software release, an SM may be specified for this option. The output is restricted to only those ISUP trunks that terminate on the specified SM.

The `OP:SS7` output message also provides a completion report to inform the user if the output has completed successfully or if the output was stopped because of a failure which prevented the output processing from continuing.

This feature also introduces the `STP:SS7` input message, which can be used to stop a currently-running `OP:SS7` request.

For further information on these messages, refer to `OP:SS7` and `STP:SS7` in the 235-600-700, *Input Messages Manual* and `OP:SS7` in the 235-600-750, *Output Messages Manual*.

5.5.6 Assignment Dependencies And Limitations

The SS7 trunk groups must contain only SS7 trunks because of the translation and recent change restrictions. The smallest unit of ISUP in a switch office is a trunk group.

5.6 OPERATIONS, ADMINISTRATION, AND MAINTENANCE

5.6.1 Maintenance Personnel Interface

The call processing subsystem interfaces with the input/output (I/O) subsystem to allow maintenance personnel to request cross-office audits of trunk related data and to allow audit results to be output to the printer.

The trunk maintenance subsystem interfaces with the I/O subsystem to allow maintenance personnel to request ISUP maintenance procedures and to see maintenance conditions.

The data base subsystem provides maintenance personnel with the ability to update and examine the ISUP data base via the I/O subsystem. The I/O subsystem provides the recent change and verify message interface needed for ISUP.

The measurement subsystem input and output messages are processed via the I/O subsystem.

5.6.2 Support Systems Interfaces

The exchanges provide a variety of operations interfaces to make them adaptable to the different operational and organizational environments. Consequently, the SS7 ISUP modifications need to be implemented at all interface points. Table 5.6-1 provides a list of all support systems that directly interface with the exchanges.

Table 5.6-1 Support Systems Interfaces

SUBSYSTEM FUNCTION ^a	AT&T SUBSYSTEM ^a	LOCAL EXCHANGE SUBSYSTEM ^a	INTERNATIONAL GATEWAY SUBSYSTEM ^a
Data Base Administration	MAC-OSS	RMAS	RC/V Terminal MFOS, Vendor's OSS
Circuit Maintenance	TOPAS CAROT RMSD2 RMSD3	#2SCCS CAROT CTTU	TOC TLWS MFOS Vendor's OSS
Measurements EADAS	MAC-OSS Printer Channel	EADAS	5ESS [®] -2000 Switch Traffic Data MFOS
Network Management ^b	EADAS/NM NEMOS		Vendor's OSS

Notes:

a. The following are definitions of terms used in this table.

CAROT - Centralized Automatic Reporting On Trunks

CTTU - Centralized Trunk Test Unit

EADAS - Engineering and Administration Data Acquisition System

MAC - Machine Administration Center

OSS - Operations Support System

MFOS - Multifunction Operations System

NEMOS - Network Management Operations Support System

RMAS - Remote Memory Administration System

RMSD2 - Remote D2 Monitoring System

RMSD3 - Remote D3 Monitoring System

2SCCS - No. 2 Switching Control Center System

TLWS - Trunk and Line Work Station

TOC - Test Operations Console

TOPAS - Testing, Operating, Provisioning, and Administration System.

- b. Network management data to and from 5ESS®-2000 switches must be initially routed via EADAS. A direct 5ESS®-2000 switch to EADAS/NM link is planned, but currently not scheduled.

5.6.3 Abnormal Operations

When an abnormal condition prevents ISUP messages from being sent to the SS7 network, SS7 trunks cannot be used; thus, a telephone user may be unable to place a call, although an SS7 trunk is idle.

5.6.3.1 Dual Seizure

Since CCS circuits may be used in two directions, it is possible that exchanges at both ends of a CCS circuit will simultaneously seize a circuit. This would be detected by an exchange receiving an Initial Address Message (IAM) for a circuit for which it had already sent an IAM. For handling cases of dual seizure, each CCS circuit should be controlled by one of the two exchanges it connects.

The ISUP protocol includes an odd/even circuit control method for resolving dual seizure. This method is applicable for both intranetwork and internetwork applications (see "ISUP Network Interconnect," Section 10 for an explanation of network interconnect). A second method for resolving dual seizure is the "all" and "none" circuit control method.

For resolving dual seizures on two-way circuits between two offices, circuit control offices are assigned. The method for assigning circuit control offices on internetwork circuit groups is determined through an agreement between the networks. A recent changeable dual seizure control indicator (See Table 5.5-1, GLARE ACTION) for each circuit group indicates the method applied. For any given circuit group, both offices apply the same method. Different circuit groups may be controlled by a different method.

When the "all/none" method is applied, a recent changeable all/none indicator for each circuit group indicates whether the office controls "all" or "none" of the circuits in the group.

The assignment of circuit control is accomplished by one of the following methods:

Odd/Even Method: The office with the highest signaling point code controls all circuits with even numbered circuit identification codes. The other office controls all circuits with odd numbered circuit identification codes.

All/None Method: One exchange controls all the circuits in a circuit group and the other controls none of the circuits in that same group. The circuit groups may be divided between offices to equalize the control responsibilities.

When a dual seizure is detected, the office uses the dual seizure control indicator and the circuit control indicator to determine if it controls the affected circuit. The office that controls the circuit proceeds to set up the call on the circuit. The non-controlling office releases any connection to the circuit and makes an automatic repeat attempt to set up a call on another circuit.

NOTE: The non-controlling office does not send an REL for the first circuit that had the dual seizure.

5.6.3.2 Unequipped Circuit Identification Code

A circuit is in the unequipped state if no valid SS7 message can be received except the transmission circuit query response, circuit validation response, or unequipped circuit identification code message. The circuit identification code is unequipped at an exchange if the code is unassigned, or if it is assigned to a circuit in the unequipped state. When an exchange receives an unequipped circuit identification code message, the circuit is taken out of service and maintenance is notified.

5.6.3.3 Additional Failure Conditions

Inability to Release: If an exchange is unable to change the circuit from the busy to idle condition in response to a received REL, it removes the circuit from service, notifies maintenance personnel, and sends a blocking message to the far-end. On receiving a blocking acknowledgement message, the exchange sends an RLC.

5.6.4 Timing and Tolerances

Table 5.6-2 provides default values or ranges for the timers associated with ISUP call setup and CCS message flow. The timer names are those defined by Bellcore. The timers that have ranges defined may be updated via Recent Change View 8.15. See 235-080-100, *Translation Guide (TG-5)*, for details on procedures for setting these timers.

Table 5.6-2 Timers

Bellcore Timer	Description	Required Value or Range
T(BLO)	When sending BLO or UBL, awaiting BLA or UBA, shorter timer used for retransmission	4-15 seconds (Default of 10)
T(BLO,l)	When sending BLO or UBL, awaiting BLA or UBA, longer timer used for abnormal procedures	1 minute
T(BLO,m)	When blocking a circuit due to a BLO and after any call is released, it is used to notify maintenance	5 minute
T(CCR)	When sending a CCR, awaiting receipt of LPA	2 sec
T(CCR,r)	When responding to a continuity check request awaiting a COT or REL	10-15 seconds (Default of 12)
T(CGB)	When sending second CGB or first CGU, awaiting CGBA or CGUA shorter timer used for retransmission	4-15 seconds (Default of 10)
T(CGB,l)	When sending second CGB or first CGU, awaiting CGBA or CGUA longer timer used for abnormal procedures	1 minute
T(COT,d)	When sending IAM requesting continuity check, delay in sending tone	50-500 ms
T(COT,r)	When receiving first COT coded "failed," awaiting receipt of CCR	16-20 seconds
T(COT)	When requesting a continuity check in an IAM awaiting return of suitable tone	2 seconds
T(CRA)	After sending CRA, awaiting IAM or REL	20-25 seconds ^{a b} (Default of 25)
T(CRM)	After sending CRM, awaiting CRA or REL	3 seconds
T(CVT)	When sending CVT, awaiting CVR	10 seconds
T(CQM)	When sending CQM, awaiting CQR	10 seconds
T(EXM,D)	After sending IAM, delay in returning EXM	100-1200 ms ^a (Default of 300)
T(g)	Guard timer on outgoing inband circuit before idling	0.75-1 seconds
T(GRS)	When sending second GRS, awaiting GRA, shorter timer used for retransmission	4-15 seconds (Default of 10)
T(GRS,l)	When sending second GRS, awaiting GRA, longer timer used for abnormal procedures	1 minute
T(IAM)	When sending IAM, awaiting ACM, ANM, or REL	20-30 seconds (Default of 25)
T(LPA,r)	When receiving an LPA, awaiting the receipt of a suitable tone and its removal	2 seconds

T(REL)	When sending REL, awaiting RLC, shorter timer used for retransmission	4-15 seconds (Default of 10)
T(REL,lj)	When sending REL, awaiting RLC, longer timer used for abnormal procedure	45-75 seconds (Default of 60)
T(RSC)	When sending RSC, awaiting response, shorter timer used for retransmission	4-15 seconds (Default of 10)
T(RSC,l)	When sending RSC, awaiting response, longer timer used for abnormal procedures	180-1800 seconds (Default of 180)
T(SUS)	When sending SUS, awaiting called party off-hook or REL	15 seconds
T(SUS,r)	When receiving SUS, awaiting calling party disconnect, RES or REL	4-15 seconds (Default of 12)
T(T)	Is not implemented but T(306) in Q.931 is used. Times deviation of audible ringing to caller.	30-150 seconds (Default of 60)
Notes:		
a. 5ESS®-2000 switch uses default value of 300 ms for T(EXM,D) and 25 sec for T(CRA).		
b. Analogous to MF total address time-out interval of 15 seconds.		

5.6.5 Message-Processing Irregularity and Trouble Event Trap

The measurements and call irregularity messages alert maintenance personnel to irregularities and trouble conditions. Message-processing irregularity and trouble event trap (user activated) are provided by the switch to collect and report detailed data on message processing irregularities or trouble events detected in the switch. The message-processing irregularity and trouble event trap are based upon existing switch capabilities, such as the direct signaling event trap.

The switch allows the maintenance personnel to activate the traps for a specified event. When the event occurs, the switch displays the relevant information about the event. The switch traps the event and displays data shown in () as follows:

- UII or ATP dropped due to ISUP maximum length violations. [Display the OPC, DPC, CIC, and trunk group/member which received or attempted to send the ISUP message with UII or ATP, the direction of ISUP message (either INCOMING to the switch or OUTGOING from the switch), the length of the ISUP message, UII length, ATP length, the ISUP message type, and the call state at the time the UII or ATP was dropped].

The following is a scenario for the use of the message-processing irregularity and trouble event trap. The maintenance personnel are alerted to trouble by a high-measurement count, such as a high-level of ISUP messages with ATP dropped. The maintenance personnel activate the particular trap via an input command, such as

```
SET:ISUP UIIATP-DROP, DUR=10;
```

The switch processes the request and outputs the trap data triggered by the trapped event. An example output could look similar to the following:

```
REPT ISUP ATP/UII
TKGMN=b-c DIRECTION=d
OPC=e DPC=f CIC=g
MSGLENGTH=h ATPLENGTH=i UIILENGTH=j
MSGTYPE=k
CALLSTATE=l
```

The maintenance personnel can use this output to sectionalize troubles (that is, to trace the call processing events within the switch). An example "sanity check" test of this feature could be to input ISUP test signaling messages with an abnormally long ATP parameter (greater than 131 octets including the parameter name and length indicator), and to activate the event trap for ATP dropped. Then, it could be verified that ATP was dropped and the

event trap had been activated properly.

5.6.6 Network Management - Automatic Congestion Control Parameter

The switch recognizes the dynamic overload control (DOC) parameter and the automatic congestion control level (ACCL) parameter in both the release and the address complete messages.

The ACCL parameter is placed in the ACM. It is not necessary to suppress this action in an access tandem or end office application.

ISUP (SS7) uses the ACCL parameter to tell surrounding offices that this office is in overload.

From Network Management's point of view, the parameters received are the same and are referred to as DOC, not ACCL parameters. When the overload indication is received, NM checks to see if there are any DOC controls assigned to the affected trunk(s). The way these controls are assigned is beforehand, usually by the remote NM center (for example, NETMINDER), but there are also on-site commands that can be used. Refer to `ASG:DOC` in the 235-600-700, *Input Messages Manual* and 235-600-750, *Output Messages Manual* for more information. If there is a control on the trunk group that received the automatic congestion control level, it is activated, and throttles traffic on the trunk group as defined by that control (it is possible to pick different percentages, different types of traffic to control, and Skip or Cancel). The control deactivates 3 to 6 seconds after the last automatic congestion control level is received.

NOTE: There is a danger that some switches may treat the ACCL parameter as unrecognized and pass it to a preceding exchange resulting in false information. From a remote center or on site, it is possible to inhibit sending these overload notifications out using the following: `INH:DSILC`.

An ACCL with *congestion level 3* indication is treated the same as an ACCL with a *congestion level 2* indication. The ACCL parameter may be present and is processed in the ACM, CRB, and REL messages.

5.7 ISUP MESSAGE LOOP DETECTION (HOP COUNTER)

5.7.1 Feature Description

The ISUP Message Loop Detection (MLD) feature, 99-CP-3053, adds an Integrated Services Digital Network User Part (ISUP) parameter to count the number of switches or hops a call has traversed. This "hop counter" controls the number of hops and prevents infinite looping in the signaling network.

5.7.2 Background

The Signaling Network Systems Committee of the Federal Communications Committee (FCC) Network Reliability Council has recommended SS7 signaling enhancements. This feature is classified as a Category 2 enhancement.

The International Telecommunications Union -Telecommunication Standardization Sector (ITU-TS) (formerly CCITT) included a hop counter parameter in the ISDNUP protocol to help minimize signaling looping within the SS7 signaling network. The hop counter parameter is an extension of the ISUP protocol and is deemed a necessary upgrade to increase network efficiency and reliability.

5.7.3 Availability

This optional feature is distributed in the 5E11 software release.

This is a secured feature (SFID=163) and a right-to-use (RTU) fee must be paid to Lucent Technologies before enabling information is provided.

5.7.4 Environment

This feature is activated on a trunk group basis.

5.7.5 Feature Operation

The ISUP-MLD feature allows a hop counter parameter in the IAM message. This parameter contains the maximum number of hops (switch to switch connections) that a call may encounter.

As a call progresses through the network, and encounters the first trunk group with the hop counter active, the hop counter parameter is generated with a maximum value. When additional trunks are encountered, with the feature active, the hop counter value is decremented. When the hop counter value is exhausted the call is terminated by sending a REL message containing a cause value of 25, thus preventing looping. When the call is terminated an assert (PSRIPKT-BPATH) is printed and an SS7 REL message is sent to the preceding exchange. An assert message is also printed when a REL message is received with cause value of 25. This is a signal that the call has exceeded looping thresholds at the next switch. See 235-600-500, *Asserts Manual* for details about assert messages.

When this feature is used, if the hop count is set too low, normal calls could be rejected when the hop count reaches zero. If the count is set too high, extra resources will be used before the loop is detected. To determine the maximum number of hops considered "normal" for an ISUP IAM message in the network, the initial hop count should be greater than the maximum number of switches that a call will traverse. The maximum number of hops will be in the range 1-20, with 20 as the default.

If a call encounters a ISUP7 trunk where the feature is not activated the hop counter is passed on to the next switch.

5.7.6 User Operation

The service provider must unlock this secured feature and enable the feature using recent change procedures.

5.7.7 Engineering

5.7.7.1 Hardware Resources

No hardware considerations are associated with this feature.

5.7.7.2 Software Resources

No software considerations are associated with this feature.

5.7.7.3 Transition Considerations

There are no transition considerations associated with this feature.

5.7.8 Interactions and Limitations

The ISUP-MLD capability is most valuable when implemented on all switches in the network. Switches that do not support the hop counter parameter will not generate the parameter, but will pass the parameter without decrementing the count.

If call forwarding occurs at a switch, the received hop counter is reset to the maximum allowed for the trunk group, regardless of the ISUP MLD feature activation status, and looping is then prevented by the number of call forwardings allowed. If the hop counter was not received by the call forwarding switch, it will only be created if the ISUP MLD feature is active for the trunk.

5.7.9 Incompatibilities

There are no incompatibilities associated with this feature.

5.7.10 Dependencies

No other features need to be installed or activated in order for this feature to work.

5.7.11 Isolation Constraints

Not applicable.

5.7.12 Feature Implementation

5.7.12.1 Office Data Administration (ODA) Provisioning

There is no ODA provisioning associated with this feature.

5.7.12.2 Recent Change Provisioning

The service provider must unlock this secured feature and activate the feature using recent change procedures.

Unlock the security lock for the feature by populating Recent Change View 8.22, *Secured Feature Upgrade*:

FIELD	VALUES
FEATURE ID	163
MODULE	(OFC or SM 1-192)
PASSWD	(Obtain from Lucent Technologies SFID Administrator)
ACTIVE	Y

"Y" - Turns on (unlocks) the feature

"N" - Turns off (locks) the feature

When this feature is loaded in the switch, the feature will be turned off for all existing trunks and it must be turned on to include the "hop counter" parameter in the IAM. For all new trunks the feature will be turned on automatically when the trunk group is provisioned.

Activate the feature using Recent Change view 5.1, *Trunk Group*:

FIELD	VALUES
ISUP_MLD	Y
MAX_HOP_CNT	1-20 (default=20)

"Y" - Turns on (enables) the feature

"N" - Turns off (disables) the feature

* See 235-118-2xx, *Recent Change Reference* for detailed information on allowed values.

5.7.13 Administration

5.7.13.1 Measurements

This feature does not impact measurements.

5.7.13.2 Billing

This feature does not impact billing.

5.8 TRUNK MAINTENANCE

5.8.1 Description

The common channel signaling (CCS) trunk maintenance capability provides trunk status administration and testing of ISUP trunks used within the switch. The trunk maintenance capability provides the interface between the ISUP and trunk circuit maintenance on the switch. The ISUP trunk maintenance software provides the majority of trunk maintenance functions that currently exist on inband trunks with the additional functions designed specifically for ISUP trunks.

The CCS trunk maintenance includes the following:

- Blocking and unblocking (sending and receiving)
- Automatic continuity recheck
- Reset (sending and receiving)
- Machine detected interoffice irregularities (MDII) reporting
- Trunk testing
- Trunk/circuit query
- Trunk translation testing.

The following ISUP messages are used to administer and maintain trunk status.

- Blocking acknowledgement (BLA) message
- Blocking (BLO) message for individual circuit
- Circuit group blocking acknowledgement (CGBA) message
- Circuit group blocking (CGB) message
 - Hardware group blocking (HGB) message
 - Maintenance group blocking (MGB) message
- Circuit group reset acknowledgement (GRA) message.
- Circuit group reset (GRS) message
- Circuit group unblocking acknowledgement (CGUA) message
- Circuit group unblocking (CGU) message
 - Hardware group unblocking (HGU) message
 - Maintenance group unblocking (MGU) message
- Circuit query request (CQM) message
- Circuit query response (CQR) message

- Circuit validation test response (CVR) message
- Circuit validation test (CVT) request message
- Continuity check request (CCR)
- Loopback acknowledgement (LPA) message
- Release (REL) message for individual circuit
- Release complete (RLC) message
- Reset circuit (RSC) message for individual circuit
- Unblocking acknowledgement (UBA) message
- Unblocking (UBL) message for individual circuit
- Unequipped CIC (UCIC) message

Prior to the 5E11 software release, all ISUP trunks used an SS7 signaling platform on the common network interface (CNI). In the 5E11 software release, SM-based SS7 signaling became available in VDCX offices, and in the 5E12 software release, was generalized to any 5ESS®-2000 switch SM; see "SS7 Access on a Packet Switch Unit (PSU) Platform," Section 12, for more details. Maintenance scenarios described in the remainder of this section refer to ISUP trunks supported by *either* CNI-based or SM-based SS7 signaling platforms, unless specifically stated otherwise.

5.8.2 Availability

The trunk maintenance capabilities covered in this section are available with all software releases.

Significant enhancements in the area of circuit query and trunk translation testing were made in the 5E12 software release. These enhancements are discussed in "Circuit or Trunk Query," Section 5.8.7 and "Trunk Translation Test," Section 5.8.8, respectively.

5.8.3 Machine Detected Interoffice Irregularities (MDIIs)

A machine detected interoffice irregularity (MDII) is an abnormal event during calls using ISUP trunks, or while performing maintenance activities on those trunks. MDIIs are not produced if problems can be traced to local overload conditions or outages (such as SM isolation, or unavailability of signaling transport to the remote office). Local switch personnel will be notified by a REPT MDII output message of such abnormal events. Such abnormalities may be transient in nature, and maintenance software will provide automatic recovery. However, persistent problems may require manual intervention, as there is a high likelihood that the remote office is at fault.

Table 5.8-1 provides a list of MDIIs that are specific to ISUP trunk call processing or maintenance activities. In addition to the MDII type listed, the origination point code (OPC) associated with the local office, the destination point code (DPC) associated with the remote office, and the circuit identification code (CIC) identifying the specific ISUP trunk are provided in the output message. For a detailed description of these MDIIs, refer to the APP-MDII appendix in 235-600-750, *Output Messages Manual*.

Table 5.8-1 ISUP Specific MDIIs

MDII	DESCRIPTION
ATI	Address Complete Incoming
ATO	Address Complete Time-Out

BAF	Blocking Acknowledgement Failure
CAF	Circuit Reset Acknowledgement Failure
CAI	Received REL with Cause = 28
CII	CCS IAM Irregularity (Mutilated or Invalid Digits)
CKF	Continuity Check Failure
CQR	Circuit Query Response Failure ^a
CRA	Circuit Reservation Acknowledgement Failure
CRF	Continuity Recheck Failure
CRR	CCS Reset Received for Incoming Call
CTO	Continuity Time-Out
CVN	CCS Vacant Number Received
HGBAF	Hardware Group Blocking Acknowledgement Failure
HGUAF	Hardware Group Unblocking Acknowledgment Failure
IAD	Incomplete Address Detected
IAM	Initial Address Message Time-Out
MGBAF	Maintenance Group Blocking Acknowledgement Failure
MGUAF	Maintenance Group Unblocking Acknowledgement Failure
MRF	Message Refusal Received
RST	Reset Received On Outgoing Trunk
RTF	Sent REL, Received No RLC
SFI	Signaling Network Failing Incoming
SFO	Signaling Network Failing Outgoing
UAF	Unblocking Acknowledgement Failure - Sent UBL out, received no UBA in return
UQL	Unequipped Label Received
VPA	Outgoing Voice Path Assurance Test Failed
WBF	Channels for an incoming wideband call are on different trunk groups on the same facility.
Notes:	
a. Implemented in the 5E12 software release.	

5.8.4 Blocking and Unblocking Messages

ISUP trunk maintenance on a 5ESS[®]-2000 switch handles the sending and receiving of individual circuit and circuit group blocking and unblocking messages.

If one of more ISUP trunks are **locally blocked** (that is, removed from service manually for testing, or due to a detected fault), blocking messages are sent to the remote offices (far-end of the affected trunks). When the remote office receives the blocking message, it prohibits any new outgoing traffic on the affected trunk or trunks. If there is a stable call on the trunk to be blocked, it will be allowed to complete (if possible), but further connections are disallowed.

The sending office must mark its end of the trunk as locally blocked before a blocking message can be sent. The 5ESS[®]-2000 switch supports the following locally blocked states for ISUP trunks:

- Out-of-Service, Maintenance, Disabled (**OOS,MTCE,DSBLD**) the ISUP trunk has been manually removed from service for administrative reasons or for testing. Such trunks must be manually restored.
- Out-of-Service, Maintenance, Locked Out (**OOS,MTCE,LKDO**) this state was provided for commonality with non-CCS trunks, but is invalid for ISUP trunks.
- Out-of-Service, Maintenance, Family-of-Equipment (**OOS,MTCE,FE**) the ISUP trunk has been removed from service because parent access hardware or circuits (family-of-equipment) have been removed, either manually or due to faults. It is possible that the loss of access hardware affects multiple ISUP trunks simultaneously. Such trunks are returned to service automatically when the parent hardware is restored.
- Out-of-Service, Maintenance, Facility Failure (**OOS,MTCE,FAF**) the ISUP trunk has been removed from service because local hardware circuits have detected loss of carrier on a digital access facility. It is possible that a carrier group alarm will affect multiple ISUP trunks simultaneously. Such trunks will be returned to service automatically when the facility facility carrier group alarm is cleared.

It should be noted that ISUP trunks may possess compound OOS statuses. For example, a manually removed

ISUP may experience a carrier failure, resulting in an OOS,MTCE,FAF/OOS,MTCE,DSBLD status. Blocking messages are sent only once in this case, when a non-locally blocked trunk first becomes locally blocked. In this example, when an in-service (IS) trunk is manually removed, a blocking message is sent, but when the carrier failure is detected, the trunk is already locally blocked and no blocking message is sent for that trunk.

If more than one ISUP trunk with the same DPC, same OPC, and CICs within a range of 24 are to be blocked at approximately the same time, circuit group blocking (CGB) messages will be sent for the affected circuits. This could occur when all trunks in a trunk group are removed, or when a hardware or carrier failure affects multiple trunks.

ISUP circuit group blocking messages identify whether the blocking is due to "maintenance" or "hardware" reasons. Circuit group blocking with maintenance indicator (with the acronym MGB) is sent for trunk outages to accommodate switch personnel in maintenance routines (this includes manual trunk removals, as well as hardware loss due to manual removal or detected faults). Circuit group blocking with hardware indicator (with the acronym HGB) is sent for outages caused by a hardware detected carrier alarm only.

If trunks do not satisfy the multiple trunk in a CIC range of 24 as previously described, an individual blocking message (BLO) is sent. An exception occurs when a carrier group alarm is detected, in that an HGB is always sent, even if only one trunk is to be blocked.

Table 5.8-2 shows the stimulus, the resulting trunk status, and the type of blocking messages sent.

Table 5.8-2 Locally Blocked Status to Blocking Message Mapping

STIMULUS	TRUNK STATUS	MESSAGE SENT
Manual Trunk Removal	DSBLD, LKDO	BLO, MGB
Family of Equipment Failures	FE	MGB, BLO
Carrier Group Alarm Failure	FAF	HGB

When a 5ESS®-2000 switch receives a blocking message from the remote office (either a BLO, MGB, or HGB), the affected trunks will be placed in a **remotely blocked** state, specifically Out-of-Service, Blocked (**OOS,BLKD**). This will deny call processing access for outgoing calls on the affected trunk(s).

Analogous events occur when one or more ISUP trunks are restored to service from a locally blocked state. Unblocking messages are sent to the remote switch, so that the trunk may be used for outgoing calls at that switch.

If one or more manually removed ISUP trunks are restored, or parent hardware restoration returns one or more trunks to service, an unblocking (UBL) or circuit group unblocking (CGU) with maintenance indicator set (the acronym for this case is MGU) message is sent. The MGU is sent if more than one ISUP trunk with the same DPC, same OPC, and CICs within a range of 24 are to be unblocked at approximately the same time.

A CGU with hardware indicator set (the acronym for this case is HGU) message is always sent when the unblocking activity is due to the clearing of a carrier group alarm. This is true whether or not multiple trunks within a range of 24 CICs are identified.

Table 5.8-3 shows the stimulus, the trunk status deleted, and the type of unblocking messages sent.

Table 5.8-3 Locally Blocked Status Deletion to Unblocking Message Mapping

STIMULUS	TRUNK STATUS DELETED	MESSAGE SENT
Craft Trunk Restore	DSBLD, LKDO	UBL, MGU
Parent Hardware Restored	FE	MGU, UBL
Carrier Group Alarm Cleared	FAF	HGU

When a 5ESS®-2000 switch receives an unblocking message from the remote office (either a UBL, MGU, or HGU), the affected trunks will have the OOS,BLKD state deleted. This allows call processing to hunt the affected trunks for outgoing calls (provided there is no other local OOS status remaining on the trunk).

When one or more trunks are manually removed to an OOS,MTCE,DSBLD or OOS,MTCE,LKDO state, a RMV TRK is produced immediately in a 5ESS®-2000 switch as the locally blocked status is added to each trunk. This is not the case when parent hardware is removed or a carrier group alarm is detected; the hardware removal or carrier failure is reported on the ROP, but no RMV TRK messages are produced for affected trunks.

When transitioning to an OOS,BLKD state due to a blocking message received from the remote office, a RMV TRK message for each affected trunk is produced, if initiated by a MGB; no messages are produced for a received HGB, as the facility problem will be reported locally. If a BLO is received, the printing of the RMV TRK is delayed for five minutes; if a corresponding UBL is not received within that time, the RMV TRK message is produced.

Analogously, RST TRK messages are produced for trunks that are manually restored locally. No RST TRK messages are produced when parent hardware is restored or a carrier group alarm is cleared, but switch personnel are made aware of the hardware or carrier restoration.

When a MGU is received from the remote office, RST TRK messages are printed for all affected trunks; no messages are produced for a received HGU, as the clearing of a facility failure will be reported locally. If a UBL is received, the RST TRK message is produced only if the trunk was remotely blocked more than five minutes; if within the five-minute interval, no RST TRK is produced (as there was no corresponding RMV TRK message printed).

Figures 5.8-1 and 5.8-2 illustrate the sequence for locally blocking and unblocking an individual trunk, and the interaction between the near-end and far-end 5ESS®-2000 switches.

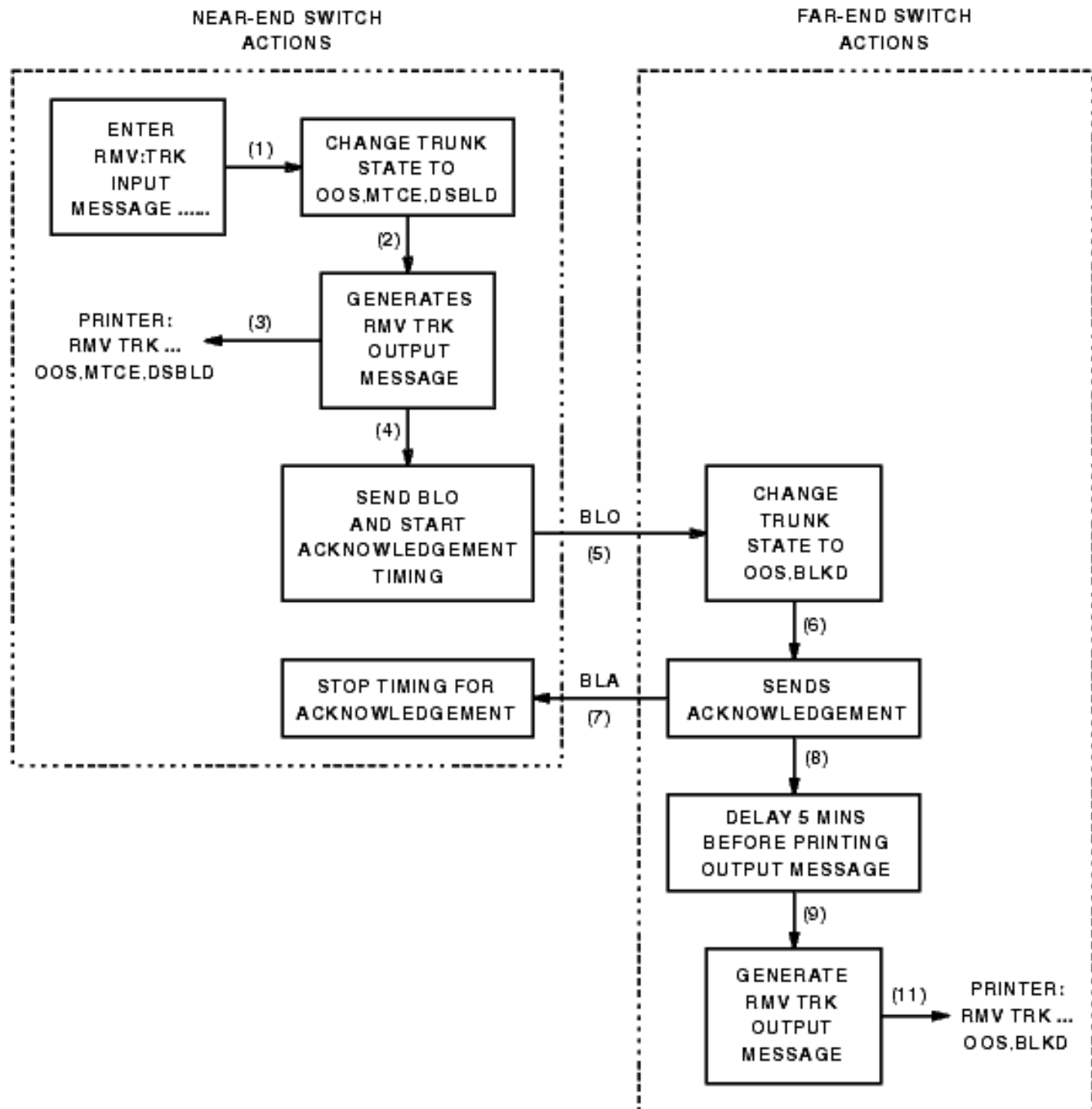


Figure 5.8-1 Trunk Blocking Sequence

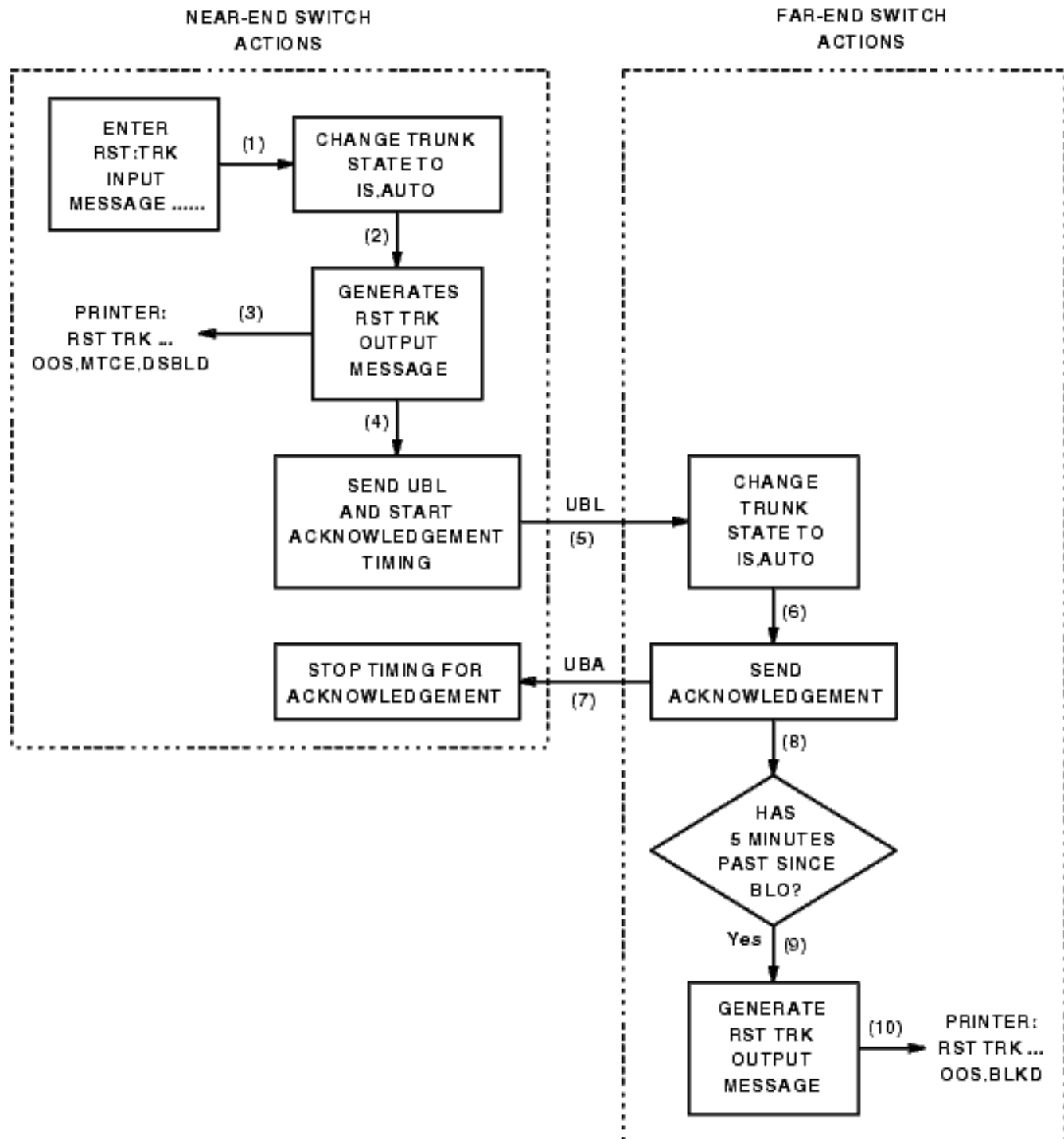


Figure 5.8-2 Trunk Unblocking Sequence

The remote office must acknowledge all blocking or unblocking messages received. For individual trunks, this is a blocking acknowledgment (BLA) or unblocking acknowledgment (UBL). For group requests, this is the circuit group blocking acknowledgment (CGBA) or circuit group unblocking acknowledgment (CGUA).

The circuit group blocking or unblocking acknowledgement message is returned only after all trunks specified in the circuit group message have been processed.

The sending switch must repeat sending the message, if an acknowledgment is not received within a timing interval. If the receiving office does not acknowledge, the sending switch must resend the blocking/unblocking message to every 4 to 15 seconds (recent changeable cycle time) for a period of 1 minute.

After 1 minute, a REPT MDII output message is printed to notify the maintenance personnel about the unacknowledged message. Table 5.8-4 contains MDII messages mapping to blocking/unblocking message failures.

Table 5.8-4 MDII Messages Printed When Acknowledgement Message Not Received

BLOCKING/UNBLOCKING MESSAGE	MDII ^a
BLO	BAF
UBL	UAF
HGB (CGB with hardware indicator)	HGBAF
HGU (CGU with hardware indicator)	HGUAF
MGB (CGB with maintenance indicator)	MGBAF
MGU (CGU with maintenance indicator)	MGUAF
Notes:	
a. BAF and UAF MDIIs are also produced when a group blocking or unblocking acknowledgment is received, respectively, but all the referenced trunks are not processed.	

Finally, switch personnel can remove an ISUP trunk to a special Out-of-Service, Circuit Administration, Disabled (**OOS,CADN,DSBLD**) state for administrative purposes; also, newly provisioned trunks leave recent change in the OOS,CADN,DSBLD state. This is a powerful state that is not affected by parent hardware removals or carrier failure, and even survives full SM initializations. The only way to delete this state is to issue a manual RST:TRK request with appropriate state options.

With respect to blocking or unblocking activities, the OOS,CADN,DSBLD trunk also reacts differently, as this state normally is associated with trunk growth/degrowth, which is monitored closely by switch personnel. When a trunk is removed to an OOS,CADN,DSBLD state, no blocking message is sent; analogously, when it is restored, no unblocking message is sent. If a blocking or unblocking request is received from the remote switch for such a trunk, no BLA/UBA is returned for individual requests, or CGBA/CGUA returned include an indication that the requested processing for any OOS,CADN,DSBLD trunks was unsuccessful.

5.8.5 Continuity Recheck Request

If a continuity check fails during call setup, a VPA MDII is printed in the outgoing office and control of the trunk is given to the trunk maintenance to perform a recheck (normally 5 seconds later). If the recheck fails, the both ends of the trunk are taken out of service and RMV TRK output messages are printed to notify maintenance personnel in both the near-end and far-end 5ESS[®]-2000 switch offices. The near-end office trunk is put in the Out-of-Service, Maintenance, Continuity Failure, Outgoing (OOS,MTCE,CONT,OTG) status. The far-end office trunk is put in the Out-of-Service, Maintenance, Continuity Failure, Incoming (OOS,MTCE,CONT,INC) status.

Periodic continuity rechecks (normally at 2-minute intervals) will be performed on the trunk until the continuity test passes or switch personnel intervene. Test scheduling and test execution are done at the request of the OOS,MTCE,CONT,OTG end of the trunk. When a subsequent continuity recheck passes, the trunk is restored to service by removing the OOS,MTCE,CONT status at both ends of the trunk and a RST TRK message is printed to notify maintenance personnel. If the OOS,MTCE,CONT,INC does not receive a request to perform a continuity check every 3 minutes, it will abandon continuity recheck and restore the trunk to service.

Maintenance personnel can also perform a continuity check by manually making a test call (TST-TRK input message).

The maintenance personnel can stop an automatic recheck cycle by an RMV-TRK input message to remove the OOS,MTCE,CONT,OGT status. Figure 5.8-3 is a diagram showing the continuity recheck sequence.

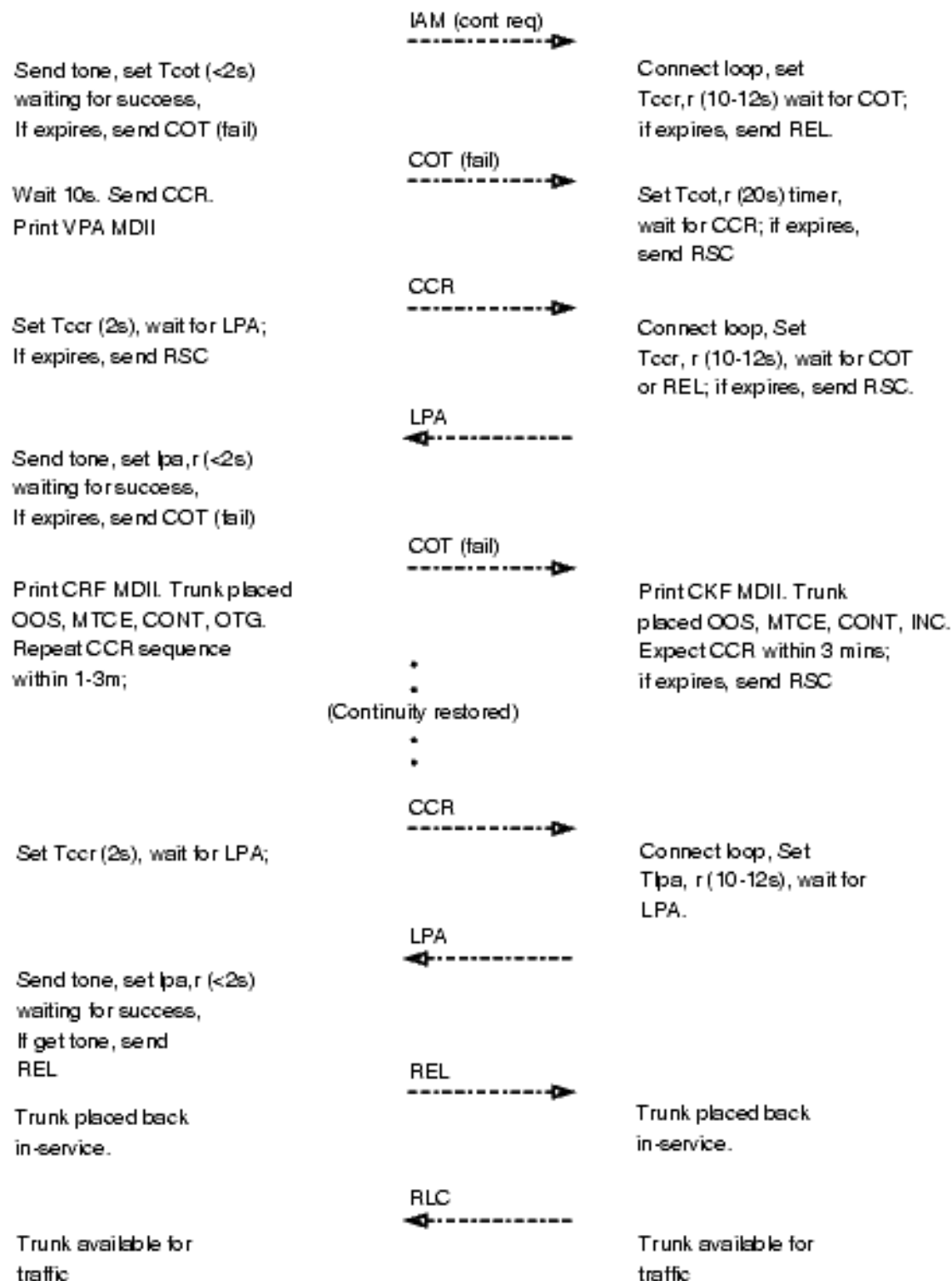


Figure 5.8-3 Continuity Recheck Sequence

5.8.6 Reset Messages

A reset circuit (RSC) message is sent to connecting office to restore a single trunk to the idle condition. A group reset message (GRS) is sent to connecting offices to restore a range of trunks to the idle condition. The exchange

sending an RSC must wait until a release complete (RLC) message is received from the far-end office before idling the trunk. The exchange sending a GRS must wait until a group reset acknowledgment (GRA) is received.

A typical example is when an RLC is not received during a disconnect, or when a call has lost sanity due to the reception of an unexpected message. In this case, the local 5ESS[®]-2000 switch will send an RSC to the remote switch, expecting an RLC acknowledgment within a timing interval. If the RLC is received, the affected trunk becomes available for hunting. If, however, the remote office does not respond, the local switch must resend the RSC every 4 to 15 seconds (recent changeable), until an RLC is received or 1 minute elapses. At this time, a REPT MDII of type **CAF** is printed, and the trunk state changes to Out-of-Service, Maintenance, CCS Initialization (**OOS,MTCE,CCSINIT**). From this point, an RSC is sent for the OOS,MTCE,CCSINIT trunk on a 1 minute interval, until an RLC is received (which causes the trunk to be returned to an IS and idle condition), or the trunk is removed to a different state.

Similarly, when a GRA is not received during a wide-band call disconnect, or when a wide-band call has lost sanity, the local 5ESS[®]-2000 switch will send a GRS to the remote switch, expecting a GRA acknowledgment within a timing interval. If the GRA is received, all trunks associated with the wide-band call become available for hunting. If, however, the remote switch does not respond, the local switch must resend the GRS every 4 to 15 seconds (recent changeable), until a GRA is received or 1 minute elapses. At this time, a REPT MDII of type **CAF** is printed, and the state of all affected trunks changes to OOS,MTCE,CCSINIT. From this point, a GRS is sent for the OOS,MTCE,CCSINIT trunks on a 1 minute interval, until a GRA is received or the trunks are removed to a different state.

Also, when a 5ESS[®]-2000 switch SM undergoes a full initialization, all ISUP trunks are placed in an OOS,MTCE,CCSINIT state (unless they are OOS,CADN,DSBLD). Similarly, transient calls torn down during an SM selective initialization, or detailed audit errors, result in ISUP trunks being placed in an OOS,MTCE,CCSINIT state. For such trunks, an RSC or GRS will be sent; GRSs will be sent if possible (for OOS,MTCE,CCSINIT trunks with the same OPC and DPC, and with contiguous CICs in the same range of 24), and GRS are always sent in pairs within a 5-second interval. If the acknowledgment (RLC or GRA) is not received within a time-out interval, retries will occur at 1-minute intervals.

It is possible that problems in the remote office make the reset of its end of the trunk impossible (even though acknowledgments can be sent). In this case, when an RSC is received by the remote office, it returns an RLC, immediately followed by a BLO; the result is that the trunk transitions to an OOS,BKLD state. Similarly, if a GRS is sent, the remote office returns a GRA, with an encapsulated "bit field" specifying one or more trunks have not been successfully reset; trunks identified are placed in an OOS,BKLD state.

On a 5ESS[®]-2000 switch, the following event occurs when a reset is received:

- If an RSC or GRS is received on a trunk supporting a call, the call is disconnected, returning the trunk to an IS and idle state. Also, a REPT MDII message is printed (type CRR for a reset incoming call, or type RST for a reset outgoing call).
- If an RSC is received for a locally blocked or OOS,CADN,DSBLD trunk, an RSC response will be sent, followed immediately by a BLO message to resynchronize status in the remote office. If a GRS is received in this case, a GRA will be returned with the appropriate "bit field" configuration as previously described.

Finally, in a 5ESS[®]-2000 switch, trunks in an OOS,MTCE,CCSINIT state have special properties, specifically:

- If an IAM for a new call is received, the call will be set up, and the trunk transitions to an IS state.
- If a reset is received, an acknowledgment is returned, and the trunk transitions to an IS state.
- If a BLO or UBL is received, it is not acknowledged; if a CGB or CGU is received, the "bit field" in the CGBA or CGUA returned indicates no action was taken. In these cases, the reset (which will ultimately be scheduled)

will resynchronize status with the remote office.

- The OOS,MTCE,CCSINIT state is "durable." If a trunk in this state is manually removed, OOS,MTCE,CCSINIT will be retained as a secondary state (trunk transitions to a OOS,MTCE,DSBLD/OOS,MTCE,CCSINIT state). Similarly, removal of parent hardware or a facility carrier failure result in an OOS,MTCE,FE/OOS,MTCE,CCSINIT or an OOS,MTCE,FAF/OOS,MTCE,CCSINIT state, respectively. This effectively inhibits reset activity temporarily. When the trunk is manually restored or hardware/facility problems are resolved, the trunk returns to the OOS,MTCE,CCSINIT state, and periodic reset activity resumes.

5.8.7 Circuit or Trunk Query

5.8.7.1 Introduction

The circuit or trunk query activity ensures that the near-end and far-end call processing and maintenance states of an ISUP trunk circuit are consistent and accurate.

The test is run independently of call processing or maintenance states. This test does not "use" the trunks, but simply verifies data related to the trunks and corrects inconsistencies.

The sections that follow describe details of the query process in a 5ESS®-2000 switch, and reflect extensive changes in the craft interface introduced in the 5E12 software release.

5.8.7.2 Trunk Query Audit (5E11 Software Release)

Circuit (or trunk) queries are initiated by an office by sending a circuit query request (CQM) to the remote office, requesting call processing and maintenance status for one or more trunks. A single CQM can request status for up to 24 trunks with the same OPC, DPC and contiguous CICs. The remote office returns the requested status data via a circuit query response (CQR) message. It is the responsibility of the office requesting the query to take action to correct any inconsistencies found.

In the 5E11 software release, a 5ESS®-2000 switch office executes trunk queries automatically on a continuous basis, for all statically allowed trunks in the office (see the following description of the recent change interface). The interval between individual CQMs is recent changeable by setting the TRK QRY AU field on RC/V view 8.15.

Trunk queries are allowed or inhibited *statically* on a trunk group (TG) basis, by setting the TRK QUERY field on RC/V view 5.1. A *static* query inhibit on a TG basis not only skips those trunks in the automatic office-wide query activity described previously, but also causes manually-initiated queries (described immediately following) to be denied.

The automatic office-wide query can also be allowed or inhibited *dynamically*, using the input messages:

- `ALW:CCSTQ` provides a mechanism to allow automatic office-wide trunk query.
- `INH:CCSTQ` provides a mechanism to inhibit automatic office-wide trunk query.
- `OP:CCSTQ` provides a mechanism to determine the dynamic inhibit/allow status of automatic office-wide trunk query (after an AM initialization, office-wide query is allowed by default).

Switch personnel also have the ability to *manually* request a trunk query audit for a specific trunk by issuing the `AUD:CCSTQ` command. The CQM associated with this request will encompass CICs in a range of 16 that includes specified trunk.

Regardless of the source of a query (automatic or manual), the consistency checks made and the recovery action is

identified. Switch personnel are notified of any corrective actions taken through an AUD:CCSTQ output message. State consistency does not necessarily mean state equivalence, but rather that the states at each end of the trunk complement each other logically.

Table 5.8-5 illustrates state information that may be encountered when encoding CQRs, and their meaning in a 5ESS®-2000 switch office.

The corrections provided are listed in Tables 5.8-6, 5.8-7, and 5.8-8. It should be reiterated that the corrective actions listed are initiated by the local 5ESS®-2000 switch *only* if the trunk query was spawned locally. State changes will be reported to switch personnel through the RMV TRK or RST TRK messages. If the query originates from the remote switch, only status information (from Table 5.8-5) will be encoded in the CQR for the target trunks.

Table 5.8-5 Query Statuses

STANDARD ACRONYM	STATE TYPE ^a	DESCRIPTION	5ESS®-2000 SWITCH PORT STATUSES
UNQ	N/A	Unequipped	Trunk not provisioned in office
ACT	MTCE	Active (or in-service)	IS
RBO	MTCE	Remotely blocked	OOS,BLKD
LBO	MTCE	Locally blocked	OOS,MTCE,DSBLD OOS,MTCE,FE OOS,MTCE,FAF OOS,CADN,DSBLD (for query)
LRB	MTCE	Locally and remote blocked	See LBO/RBO
TRN	MTCE or CP	Transient ^b	IS,AUDIT OOS,MTCE,COT OOS,MTCE,CCSINIT ^c
IDL	CP	Idle trunk	N/A
ICB	CP	Busy trunk (incoming side of call) ^d	N/A
OGB	CP	Busy trunk (outgoing side of call) ^d	N/A
Notes: a. STATE TYPE is MTCE for maintenance states, or CP for call processing states. b. State is owned by maintenance process or involved in TLWS activity, state is unstable, call is in process of being established or disconnected, or in special states listed. c. OOS,MTCE,CCSINIT may be a primary or secondary state. d. Trunk may be busy supporting an ordinary call or test call.			

Table 5.8-6 Transient and Unequipped State Corrections

LOCAL 5ESS®-2000 SWITCH STATE	REMOTE SWITCH STATE		
	TRN	UNQ	OTHER
TRN	No action	No action	No action
Other	No action	Idle trunk. Add OOS,CADN,DSBLD	See Tables 5.8-7 and 5.8-8

Table 5.8-7 Maintenance State Corrections

LOCAL 5ESS®-2000 SWITCH STATE	REMOTE SWITCH STATE			
	ACT	RBO	LBO	LRB
ACT	Consistent states	Send UBL	Add OOS,BLKD	Send UBL Add OOS,BLKD
RBO	Delete OOS,BLKD	Send UBL Delete OOS,BLKD	Consistent states	Send UBL
LBO	Send BLO	Consistent states	Send BLO ^a Add OOS,BLKD	Add OOS,BLKD ^a

LRB	Send BLO Delete OOS,BLKD	Delete OOS,BLKD	Send BLO	Consistent states
Notes: a. This action is not taken if locally blocked state in 5ESS®-2000 switch office is OOS,CADN,DSBLD.				

Table 5.8-8 Call Processing State Corrections

LOCAL 5ESS®-2000 SWITCH STATE	REMOTE SWITCH STATE		
	IDL	ICB	OGB
IDL	Consistent states	Send REL	Send REL
ICB	Idle trunk	Send REL Idle trunk	Consistent states
OGB	Idle trunk	Consistent states	Send REL Idle trunk

5.8.7.3 Circuit Query (5E12 and Later Software Releases)

In the 5E12 software release, circuit query functionality is essentially unchanged from previous releases except that the craft interface has changed (input messages allow more flexibility and output messages provide more detail). To avoid confusion with the previous *trunk query audit* request, the new versions of messages refer to *circuit query*; AUD:CCSTQ, INH:CCSTQ, ALW:CCSTQ, and OP:CCSTQ messages are nonfunctional in the 5E12 and later software releases.

Automatic circuit queries are still scheduled on an office-wide basis, with the following constraints:

- The CKT QUERY field on RC/V view 5.1 *statically* specifies whether or not automatic or manual queries are allowed for a specific trunk group.
- Circuit queries are executed once a day for all *statically* allowed trunks in the office. The query starts at the time specified in the CQ START TIME field on RC/V view 8.15. The time selected is in the range 0-23, corresponding to the hour on a 24-hour clock, with the default being 3:00 a.m.; a *NULL* entry will turn off all automatic queries (this is not recommended). The actual start time will be skewed by each office (from 0-10 minutes, uniquely determined by the office OPC) to avoid network saturation by query requests spawned by 5ESS®-2000 switch offices.
- Automatic queries may be *dynamically* inhibited (using the INH:CCSCQ input message) or allowed (using the ALW:CCSCQ input message). Current inhibit/allow status is obtained by the OP:CCSCQ input message, noting the default is *allow* after an AM initialization. These *dynamic* statuses have no effect on manually requested queries.

Switch personnel have the ability to manually request a circuit query for one or more trunks, using the EXC:CCSCQ input message. The following description highlights the scope of this command, but it is strongly urged that switch personnel familiarize themselves with detailed input and output formats described in 235-600-700, 5ESS®-2000 *Switch Input Messages Manual* and 235-600-750, 5ESS®-2000 *Switch Output Messages Manual*.

- The *scope* of the circuit query request using the EXC:CCSCQ input message can be the entire office, all trunks with the same OPC and DPC terminations, all trunks in a trunk group (TG), or a single trunk.

Up to 4 simultaneous query requests may be executing at once, with two caveats. If an office-wide circuit query job is running (either automatic or manual), no further query requests will be honored, and any new query request must not involve an OPC/DPC pair of a query that is already running.

- Currently running circuit query jobs may be determined by issuing a OP:JOBSTATUS, JOB=TLWS input request.
- As some circuit query jobs can take a long time to complete, any running query may be stopped gracefully by issuing a STP:CCSCQ input message, with parameters indicating the specific query to be halted. An option on

the `STP:CCSCQ` command is available to provide summary reports at the time of termination.

The queries may also be abruptly aborted using the `ABT:TASK, JOB=TLWS, PID=xxx` input message, where `xxx` is the process identifier of the target query obtained by an `OP:JOBSTATUS` output.

- An option on the `EXC:CCSCQ` input message allows switch personnel to select whether corrective action is taken, should state inconsistencies occur between the local and remote ends of the trunk. By default, corrective action will be taken.
- Switch personnel, in some cases, can choose the type of output report. The following forms are available:
 - *SHORT* form provides a count of the state consistency matches or mismatches and undetermined responses on an OPC-DPC basis. This is the only output produced in an automatic or manual office-wide circuit query. It is the default for OPC-DPC pair or TG query, and may be specified as an option on the single trunk query. This data is produced for all circuit query requests, even if more detailed output is provided.
 - *LONG* form provides detailed output (trunk group/member, OPC, DPC, CIC, near-end/far-end states, and corrective action), only for trunks where a mismatch occurs. It is available as an option for circuit queries with OPC-DPC pair, TG, or individual trunk as the scope.
 - *EXPANDED* form provides the same information as the *LONG* form, but is produced whether or not mismatches are detected. This is the default for an individual trunk circuit query, and may be specified as an option for the TG scope.
- Corrective actions listed in Tables 5.8-6, 5.8-7, and 5.8-8 are consistent with the new circuit query requests, with the exception that an OOS, CADN, DSBLD trunk or a trunk supporting a test call is now considered transient (rather than locally blocked or busy, respectively).

5.8.8 Trunk Translation Test

Trunk translation testing in a 5ESS®-2000 switch office has two components to verify that intra-switch and inter-switch static data is consistent, such that a call may be placed on a specific trunk circuit, specifically:

- An intra-office static ODD audit is executed to verify the consistency of all tuples associated with a specific trunk necessary to successful maintenance and call processing activities in the AM, CMP, and SM are consistent.
- An inter-office audit of static data is accomplished through the exchange of circuit validation test (CVT) and circuit validation response (CVR) messages. The originating CVT causes the receiving office to return specific data defined in standards (described immediately following).

Maintenance personnel in the local office can initiate such a test for a single trunk using the `AUD:CCSXLATE` command in offices loaded with a 5E11 software release, or `EXC:CCSXLATE` for offices loaded with a 5E12 or later software release. The differences in the two commands is basically reflected in the outputs produced. The CVT/CVR exchange can also be triggered by the remote office. This testing is particularly useful after network routing is established, but before a trunk is restored to service. Any problems identified involve static data, and, therefore, require switch personnel intervention in one or both offices to resolve.

The inter-office data returned in a CVR is enumerated in Table 5.8-9.

Table 5.8-9 Data Transmitted in a CVR

ABBREVIATION	DESCRIPTION	ALLOWED VALUES
CGC	Circuit group carrier indicator	analog, digital, analog and digital, unknown
DSC	Double seizing control indicator	no circuit control, odd circuit control, even circuit control, all circuit control
ACI	Alarm carrier indicator	software carrier handling, hardware carrier handling, unknown
CCI	Continuity check requirements indicator	none, statistical, per-call
CIN	Circuit identification name	digit string
CLLI	Common language location code	alphanumeric string

Of the six indicators returned in a CVR, only three can have an impact on call processing and need concern maintenance personnel, specifically:

- The near-end and far-end CGC will be reported (unless they are unknown). A CGC mismatch in itself will not impact call processing, as various offices interpret this variable according to different criteria.
- For two-way trunks *only*, the DSC values must complement each other, or call failures could occur in glare situations. *No* circuit control and *all* circuit control are consistent, as are the pair *odd* and *even* circuit control. For one-way trunks, DSC values have no impact on operation.
- ACI values are subject to individual office interpretation and do not impact call processing (the value is always considered *unknown* on a 5ESS®-2000 switch).
- CCI values have no impact on call processing, and are included for information only (value indicates the use of a default continuity test on call setup).
- The CIN is composed of the trunk's 4-digit circuit identification code (CIC), followed by the CLLIs of the near-end and far-end offices; the ordering of the CLLIs can be impacted by the trunk type (one-way or two-way trunks). The CIC or one/both CLLIs are not required to be returned in the CVR, often making CIN comparisons difficult or impossible. If all data is returned, only two facets can impact call processing: the CICs must be identical (to complete a call), and the ordering of CLLIs, if known, must be the same (or trunk types are mismatched). The actual CLLI values have no impact on call processing.
- The CLLI of the far-end office may be returned in the CVR (optional data); the local 5ESS®-2000 switch may have a copy of the *far-end CLLI* (also optional). If available, the data will be reported, but CLLI mismatches have no impact on call processing.

When a translation test is scheduled locally in a 5ESS®-2000 switch office using an `AUD:CCSXLATE` (pre-5E12 software release) or `EXC:CCSXLATE` (5E12 and later software release) command, the intra-office static ODD audit for the specified trunk is executed first. Only if this audit passes is a CVT sent to the remote office, and the CVR contents evaluated. Switch personnel are notified of the OPC, DPC, CIC, and ODD relation associated with a failed intra-office audit, or discrepancies in inter-office data; the exact output produced depends on the input command used. Consult 235-600-750, *5ESS®-2000 Switch Output Messages Manual* for details.

If a CVT from a remote switch is received by a 5ESS®-2000 switch, a CVR will be populated and returned to the remote office for evaluation. In addition, in 5E12 and later software releases, an intra-office audit will be executed locally for static ODD associated with the specified trunk (a `REPT MANUAL ACTION ASSERT` will be produced for any audit inconsistencies found).

5.8.9 Outgoing and Incoming Test Calls

The CCS trunk maintenance supports all existing trunk test capabilities that were practical for out-of-band signaling facilities.

In addition to tests that exist for inband signaling trunks, a continuity check test (voice path assurance) is used for

CCS trunks. This test may be performed on demand or by automatic progression testing. Table 5.8-10 contains information concerning supported trunk test calls.

Table 5.8-10 Supported ISUP Trunk Test Calls

FEATURE	REQ'D FOR	
	NON-CCS	CCS
Transmission and Operational Test		
Calls and Test Lines		
100	Yes	Yes
102	Yes	Yes
103	Yes	No
104	Yes	Yes
105	Yes	Yes
108 ^a	Yes	Yes
Permanent Busy	Yes	Yes
Synchronous	Yes	No
Non-Synchronous	Yes	No
Continuity	No	Yes
Automatic/Routine		
Tests (APT)		
PERM BUSY	Yes	Yes
SYNCHR	Yes	No
NON-SYNCHR	Yes	No
Continuity	No	Yes
103	Yes	No
External Test System		
Interfaces		
CAROT	Yes	Yes
ROTL	Yes	Yes
CTTU	Yes	Yes
Notes:		
a. Non-inverted loop back test line		

Normal call processing set up procedures are followed to establish a test call connection to another office. After the ANS message is received, the test call sequence is executed over the voice path. At the conclusion of the test call, normal call processing disconnect sequence is used to idle the connection.

5.8.10 Trunk and Line Work Station

The trunk maintenance capability includes changes required to interface with the trunk and line work station, and the centralized trunk test unit. Table 5.8-11 contains the features of the trunk and line work station and identifies those features that require modification for CCS application.

Table 5.8-11 Trunk and Line Work Station Features

FEATURE	REQ'D FOR	
	NON-CCS	CCS
Test Tone - At Specified Frequency and Level	Yes	Yes
Transmission Measurements - Level, Noise, and Loss	Yes	Yes
Electrical Measurements - Voltage, Resistance, and Capacitance	Yes	Yes
Monitor - Send Supervision	Yes	Yes
AC, DC, and Jacks - For Connecting to Portable Test Equipment	Yes	Yes
Wink - Send Wink and Quick Wink	Yes	No
Talk and Monitor	Yes	Yes
101 Test Line - Incoming	Yes	Yes

101 Test Line - Outgoing Test Call Setup	Yes	Yes
Trunk Status Administration	Yes	Yes

5.8.11 ISUP Signaling During SM Initialization and Isolation for CNI Trunks

As an SM enters full initialization, selective initialization, or isolation, blocking messages (individual or group) are sent to remote offices for all resident trunks using the common network interface (CNI) as a signaling platform; no blocking is sent for trunks being grown (OOS,CADN,DSBLD state). These messages are sent from the AM (and do not rely on a non-functional or isolated SM). These blocking messages are sent to remote offices, such that these offices may select ISUP trunks on other SMs or other point codes while the SM is unavailable.

When an SM exits full initialization, all ISUP trunks (except OOS,CADN,DSBLD trunks) are placed in an OOS,MTCE,CCSINIT state as described in "Reset Messages," Section 5.8.6 . This will trigger the sending of reset circuit or group reset messages to the remote office to resynchronize trunk statuses. Until appropriate reset acknowledgments are received, no outgoing calls may be attempted on the affected trunks.

When the SM recovers from a selective initialization, unblocking messages (individual or group) are sent for all traffic-capable trunks. This is to make CNI-controlled trunks available in the remote office, as they were blocked as the SM entered full initialization. During a selective initialization, all transient ISUP calls will be torn down, and those trunks will be placed in an OOS,MTCE,CCSINIT state; recover of these trunks is through the reset mechanism described in "Reset Messages," Section 5.8.6 .

When an SM exits isolation, unblocking messages (individual or group) will be sent for all traffic-capable *CNI-controlled* trunks, as they were blocked as the SM entered isolation.

The previous descriptions are valid for ISUP trunks controlled by a *CNI* signaling platform. In the 5E11 and later software releases, ISUP trunks can be supported in 5ESS®-2000 switch Very Compact Digital Exchange (VCDX) offices using SM-based signaling on a packet switch unit (PSU) platform. In the 5E12 and later software releases, these PSU signaling platforms are available for use in any 5ESS®-2000 switch SM. Because of subtle differences in signaling capabilities (PSU platform signaling is lost when the SM enters full or selective initialization, but is fully functional during isolation), philosophies are somewhat different for ISUP trunks controlled by such signaling platforms. See "ISDN User Part Services Provided," Section 12.1.6 , for a description of ISUP trunk activity during SM initialization or isolation, when PSU platform signaling is used.

5.9 VOICE PATH ASSURANCE TEST CONSIDERATIONS

Execution of the voice path assurance test is driven from the office data for the trunk group. Recent Change View 5.1 has a VPA TYPE field which is populated based by data administrators. The appropriate value to choose depends on the near office type and the far office type to determine tone frequencies to be used in running the vpa test. In addition, it involves consideration for the type of facility used and the planned ICL loss value for that facility. This information is used to control the VPA Receiver operate and release levels. The loss on the trunk affects the power level of the tone that is detected by the VPA receiver. Note that the last character of the symbol put on the recent change screen is the hardware loss threshold level. Tables 5.9-1, 5.9-2, 5.9-3, 5.9-4, and 5.9-5 show the meaning of each hardware loss threshold level.

Table 5.9-1 VPA Loss Threshold Level

Near End Office Type ^a	Far End Office Type	Trunk Facility	Trunk ICL	VPA Type
4-wire	4-wire	4-wire	0 db	4W4WL0
4-wire	4-wire	4-wire	0.1 - 0.8 db	4W4WL1
4-wire	4-wire	4-wire	0.9 - 1.7 db	4W4WL2
4-wire	4-wire	4-wire	1.8 - 2.9 db	4W4WL3
4-wire	2-wire	2-wire	0.0 - 4.0 db	4W2WL3
4-wire	2-wire	2-wire	4.1 - 5.5 db	4W2WL4
4-wire	2-wire	2-wire	4.1 - 5.5 db	4W2WL5
			HI LOSS	
2-wire	4-wire	4-wire	0 db	2W4WL0
2-wire	4-wire	4-wire	0.1 - 0.8 db	2W4WL1
2-wire	4-wire	4-wire	0.9 - 1.7 db	2W4WL2
2-wire	4-wire	4-wire	1.8 - 2.9 db	2W4WL3
2-wire	2-wire	2-wire	0.0 - 4.0 db	2W2WL3
2-wire	2-wire	2-wire	4.1 - 5.5 db	2W2WL4
2-wire	2-wire	2-wire	4.1 - 5.5 db	2W2WL5
			HI LOSS	
Notes:				
a. Used for frequency specifications only. The 5ESS®-2000 switch is always a 4-wire switch with respect to its transmission characteristics.				

Table 5.9-2 VPA Hardware Threshold Level

Hardware Level	Operate Threshold ^a	Release Threshold ^b
0	-20 dbm +/- 2dbm	-27 dbm
1	-21.5 dbm +/- 2dbm	-28.5 dbm
2	-23.2 dbm +/- 2dbm	-30.2 dbm
3	-25.6 dbm +/- 2dbm	-32.6 dbm
4	-27 +/- 2dbm	-34 dbm
5	-31 dbm +/- 2dbm	-38 dbm
Notes:		
a. Tone is detected if power level is >= value shown.		
b. Tone stops being detected (released) if power level is <= value shown.		

Table 5.9-3 gives the values for a 4-wire continuity check (4-wire switch at each end and 4-wire facility between switches).

Table 5.9-3 VPA Loss Level: 4-Wire

Bell System Inserted Connection Loss	Operate Range ^a	Release Range
0 db	-18 <= N <= -6 + n dbm	N <= -27 + n dbm
0.1 - 0.8 db	-19.5 <= N <= -7.5 + n dbm	N <= -28.5 + n dbm
0.9 - 1.7 db	-21.2 <= N <= -9.2 + n dbm	N <= -30.2 + n dbm
1.8 - 2.9 db	-23.6 <= N <= -11.6 + n dbm	N <= -32.6 + n dbm
Notes:		
a. N is the absolute power level of the check tone and n is the relative power at the input of the receiver with respect to the		

zero transmission level point.

Table 5.9-4 gives the values for a 2-wire continuity check (2-wire switch at one or both ends, with no dependence on type of facility between switches).

Table 5.9-4 VPA Loss Level: 2-Wire

Bell System Inserted Connection Loss	Operate Range ^a	Release Range
0 - 4.0 db	-23 ≤ N ≤ -11	N ≤ -32
4.1 - 5.5 db	-25 ≤ N ≤ -13	N ≤ -34
4.1 - 5.5 db HI LOSS	-29 ≤ N ≤ -17	N ≤ -38
4.1 - 8.6 db 2 Wire	-27.6 ≤ N ≤ -15.6	N ≤ -36.6
4.1 - 8.6 db 2 Wire HI LOSS	-29 ≤ N ≤ -17	N ≤ -38
Notes:		
a. N is the absolute power level of the check tone and n is the relative power at the input of the receiver with respect to the zero transmission level point.		

Table 5.9-5 VPA Frequencies Used For Each VPA Type

VPA Type	Originating Test	Frequency Sent	Frequency Received	Hardware Level
NONCCS	n/a	n/a	n/a	n/a
4W4WL0	Y	2010	2010	0
4W4WL0	N	2010	2010	0
4W4WL1	Y	2010	2010	1
4W4WL1	N	2010	2010	1
4W4WL2	Y	2010	2010	2
4W4WL2	N	2010	2010	2
4W4WL3	Y	2010	2010	3
4W4WL3	N	2010	2010	3
4W2WL3	Y	1780	2010	3
4W2WL3	N	1780	2010	3
4W2WL4	Y	1780	2010	4
4W2WL4	N	1780	2010	4
4W2WL5	Y	1780	2010	5
4W2WL5	N	1780	2010	5
2W4WL0	Y	2010	1780	0
2W4WL0	N	2010	1780	0
2W4WL1	Y	2010	1780	1
2W4WL1	N	2010	1780	1
2W4WL2	Y	2010	1780	2
2W4WL2	N	2010	1780	2
2W4WL3	Y	2010	1780	3
2W4WL3	N	2010	1780	3
2W2WL3	Y	2010	1780	3
2W2WL3	N	1780	2010	3
2W2WL4	Y	2010	1780	4
2W2WL4	N	1780	2010	4
2W2WL5	Y	2010	1780	5
2W2WL5	N	1780	2010	5

6. SS7 CONVERSION - 1A ESSTM SWITCH TO 5ESS[®]-2000 SWITCH

This section is used to replace a 1A ESSTM switch that has SS7 connectivity with a 5ESS[®]-2000 switch. A separate procedure is required because of the restrictions on circuit identification code and point codes that are not used in per-trunk signaling. This section is not intended to replace procedure manual 235-105-200, *Precutover and Cutover Procedures*. The intent is to supplement it in the areas of SS7 signaling and with the assumption that the user is familiar with SS7 signaling and switch replacement.

The procedure for cutting out the 1A ESSTM switch lines can be found in 231-300-005, *Line Cutover Procedures*, Issue 3 and later issues. The 1A ESSTM switch BWM 910378 supplements Issue 3 of this document.

6.1 SS7 SIGNALING

The SS7 signaling offices are connected to a mated pair of signal transfer points (STPs) via A-links and use a unique point code to identify all nodes in a network. All trunks connecting SS7 offices are identified by a circuit identification code that is the same in both the originating and terminating offices (see Figure 6-1).

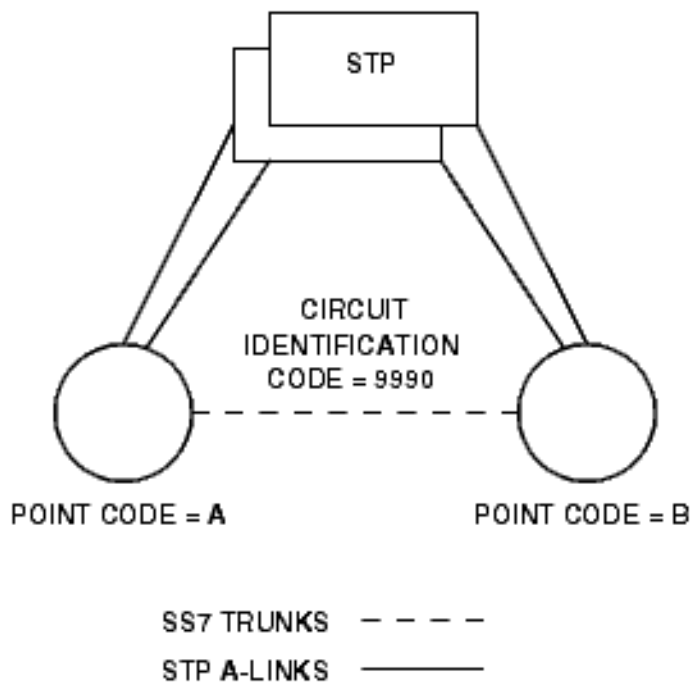


Figure 6-1 SS7 Configuration

6.2 LOCAL AREA SIGNALING SERVICES

The 1A ESSTM switch screening lists will be mapped into the 5ESS[®]-2000 switch. This procedure, along with a procedure to map other line information, is described in 235-080-100, *Translation Guide*. The line history information will not be mapped during switch replacement.

6.3 TIRKS ODA BATCH INTERFACE

The Trunk Integrated Record Keeping System (TIRKS) office data base administrator (ODA) batch interface service (referred to as TOBI) has been developed to permit direct input of TIRKS data base information, by magnetic tape, to either the 5ODA or other off-line switch-related processes. Using a TIRKS generated input data tape, the service supplies a batch interface formatted data tape to these processes. Presently, this trunk group and member data is

manually input by the customer to 5ODA from data supplied by TIRKS. The TOBI reduces the input effort and interval for the customer, improves the accuracy of the data supplied, and provides the additional interval needed to put the final touches on the error correction activity prior to the generation of the selective line and trunk translations and final office dependent data. Other processes are available that use the batch interface data to build trunk groups and members on the switch.

6.4 CUTOVER DEVICES

Cutover devices are not required for SS7 switch replacement. They may be used during trunk testing and as part of the cutover procedure. Local procedures regarding the use of cutover devices should be used.

6.5 POINT CODES

6.5.1 Office Replacement

The two fundamental methods to office replacement are as follows:

- (1) Assign a new point code to the replacement switch (which is used for capping or gradual replacement).
- (2) Use the existing switches point codes for the switch replacement (which is used for flash cut). The flash cut approach can be accomplished with no connecting office changes.

6.5.2 Assigning A New Point Code To Replacement 5ESS[®]-2000 Switch

Figure 6-2 illustrates a switch in a gradual or capping configuration. This figure shows that the switch will be in service before the retirement of the 1A ESSTM switch. This figure also shows that the 5ESS[®]-2000 switch is identified by its own unique point code with trunking between the 1A ESSTM switch and the 5ESS[®]-2000 switch. A gradual switch replacement can be done on the lines and trunks, or a flash cut can be done on the lines.

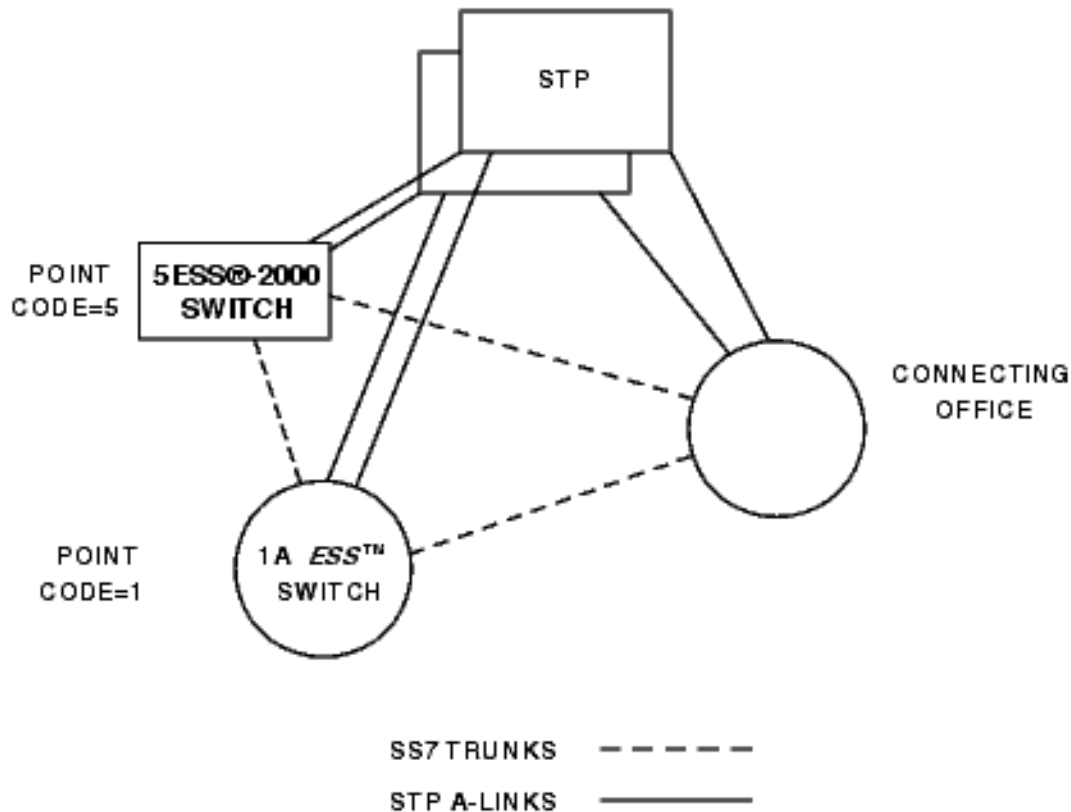


Figure 6-2 New Point Code

6.5.3 Gradual Cutover Lines And Trunks

Figure 6-2 illustrates a gradual cut procedure for lines and trunks. A portion of the lines and trunks will be moved to the replacement 5ESS®-2000 switch from the 1A ESS™ switch in several steps. Since the trunks are moved in gradually, the circuit identification code information does not need to be preserved. The SS7 trunking exists between the old and new switch. The 1A ESS™ switch procedure for line cutover is located in 231-300-005, *Line Cutover Procedures*. After the line cutover procedure is completed, the lines will be in the "precut" state with routing pointing to the 5ESS®-2000 switch. The following steps should be taken to accomplish a gradual cutover of lines and trunks to the replacing 5ESS®-2000 switch.

- (1) In the connecting offices, change the routing for the trunk group going to the 5ESS®-2000 switch (that is, add the trunk group that goes to the 1A ESS™ switch as the next route in the route list). This will act as overflow routing for the remainder of this procedure. The overflow calls will complete by using the SS7 trunks between the 1A ESS™ switch and the 5ESS®-2000 switch without a loss of local area signaling services.
- (2) In the 1A ESS™ switch, perform the line cutover procedure on the set of NXXs to be moved to the 5ESS®-2000 switch, and move the lines to the 5ESS®-2000 switch. The lines are located on the 5ESS®-2000 switch and any calls for these lines that are routed to the 1A ESS™ switch will tandem through to the 5ESS®-2000 switch.
- (3) In the STPs, alter the global title translations (GTT) for the NXXs that have been moved to show that they reside in the new point code. All queries to the NXXs are sent to the 5ESS®-2000 switch.
- (4) In the connecting offices, change the routing for NXXs that have been moved to point to the trunk group that

goes to the switch. All calls to the moved NXXs go directly to the 5ESS[®]-2000 switch.

- (5) In connecting offices and 1A ESSTM switch, remove from service the set of trunks to be moved to the 5ESS[®]-2000 switch. Use standard procedures for moving and testing the SS7 trunks. Place the trunks in service in the 5ESS[®]-2000 switch trunk group.
- (6) Repeat Steps 2 through 5 until all the lines and trunks are moved to the 5ESS[®]-2000 switch.
- (7) In the connecting offices and the STP, remove the 1A ESSTM switch point code.
- (8) Remove the A-links between the 1A ESSTM switch and the STP.
- (9) Cutover is completed.

6.5.4 Flash Cutover Of Lines For A Capped Switch

In this condition, the 1A ESSTM switch has been capped by a 5ESS[®]-2000 switch. Both switches are in service and are identified by different point codes. The 1A ESSTM switch is being retired and additional facilities will be added to the 5ESS[®]-2000 switch to handle the traffic from the retiring 1A ESSTM switch. The trunk facilities from the retiring 1A ESSTM switch will be reused in the 5ESS[®]-2000 switch after the 1A ESSTM switch is retired (Figure 6-3). The lines can be flash cut from the retiring 1A ESSTM switch to the 5ESS[®]-2000 switch, but the trunks cannot because the connecting offices identify these offices as different Destination Point Codes (DPCs) with separate trunk groups. Using the procedure, the amount of time that SS7 signaling is unavailable can be held to a minimum. There will be a longer period of time with a reduction of SS7 trunk capability, assuming that the 1A ESSTM switch trunks will be reused along with their circuit identification code information. This is done by using the Point Code Change Process (PCCP) and by partitioning the 1A ESSTM switch trunk groups that will be migrating to the 5ESS[®]-2000 switch in a subset of switch modules (SMs) [growth SMs used for replacement for the 1A ESSTM switch], while the trunk groups that are currently going to the 5ESS[®]-2000 switch will remain in the existing SMs. After the switch replacement, the trunks can be combined into one trunk group.

6.5.4.1 Point Code Change Process Description

The PCCP service changes the point code on a per-switch module basis. This is done by copying the equipment configuration data and office dependent data to a tape, using the same process as is used for a retrofit or growth order. The equipment configuration data/office dependent data tape is returned to the Network Software Center for processing. The normal interval required is 4 to 6 days and the data is returned the Monday before cutover.

During PCCP processing, SS7 trunk recent change activity must not be allowed. Changes made to SS7 trunks while the data is being processed can cause problems in the office. When PCCP outputs are returned to the site, the PCCP process depends on the on-site SS7 trunk relations data being identical to the data supplied to the PCCP. Failure to follow this requirement can cause the PCCP process to be aborted.

The PCCP process uses the Software Change Administration Notification System (SCANS) to link the changed relation data back to the site for insertion in the office dependent data (ODD). Since only the changed relations data is reloaded, a new ODD is not provided.

The PCCP process evaluates the point code change to determine if the trunk glare resolution attribute between offices must be changed. If glare resolution is required, the appropriate trunk relation data is modified.

The PCCP service can be ordered through the Network Systems Engineering Center (NSEC) that supports the office using the office record service.

The final point code that the 5ESS[®]-2000 switch assumes will depend on the amount of trunking going to the old

and new switches. If most of the trunks from the connecting offices go to the 1A ESSTM switch, the 1A ESSTM switch point code should be used to identify the 5ESS[®]-2000 switch after the 1A ESSTM switch is retired. Otherwise, the 5ESS[®]-2000 switch point code should be retained.

The circuit identification code numbers from the 1A ESSTM switch must not be reused in the 5ESS[®]-2000 switch. If the circuit identification code numbers are reused, duplicate circuit identification codes will be created when the 1A ESSTM switch trunks are moved to the 5ESS[®]-2000 switch. If the 5ESS[®]-2000 switch is identified as point code "A" and the 1A ESSTM switch is identified as point code "B," a connecting office uses circuit identification code 999 to both offices. Before the 1A ESSTM switch is retired, the system works properly. After the switch is retired (that is, one point code identifying what was formerly two offices), duplicate circuit identification codes are created.

Trunk testing before switch retirement is done either on a sampling or 100 percent basis depending on local practices.

The **pseudo-point code capability** feature described in "Pseudo-Point Code Capability Feature Description," Section 6.5.5.2 can be used for testing the 1A ESSTM switch trunks that are being reused in the 5ESS[®]-2000 switch, if the requirements of SM segregation and circuit identification code number reuse are met. The temporary point code populated in the 1A ESSTM switch should be that of the 5ESS[®]-2000 switch. The originating point code (1A ESSTM switch point code) populated in the 5ESS[®]-2000 switch trunk groups that will be used to test the reused 1A ESSTM switch trunks should be made via an ODA run or an insert of Recent Change View 5.1. The originating point code cannot be updated after the view has been inserted. To change the originating point code after testing, the PCCP must be used. The method used to turn the feature on and off in the 1A ESSTM switch is the same. The 5ESS[®]-2000 switch Recent Change View 15.1 must not be changed when turning the pseudo-point code feature on and off in the 5ESS[®]-2000 switch. Since the originating point code in the test trunk groups is different from the point code in View 15.1, pseudo-point code can be used to test these trunks when the feature is active. The trunk testing procedure described for pseudo-point code should be used. To save real time, the pseudo-point code feature must be turned off when not in use.

The 1A ESSTM switch point code is reused in the 5ESS[®]-2000 switch and trunk testing is completed. Figure 6-3 illustrates the switch configuration. It is intended as an example and does not imply that all actions should be completed in the exact order. Local practices should be consulted for any specific switch replacement.

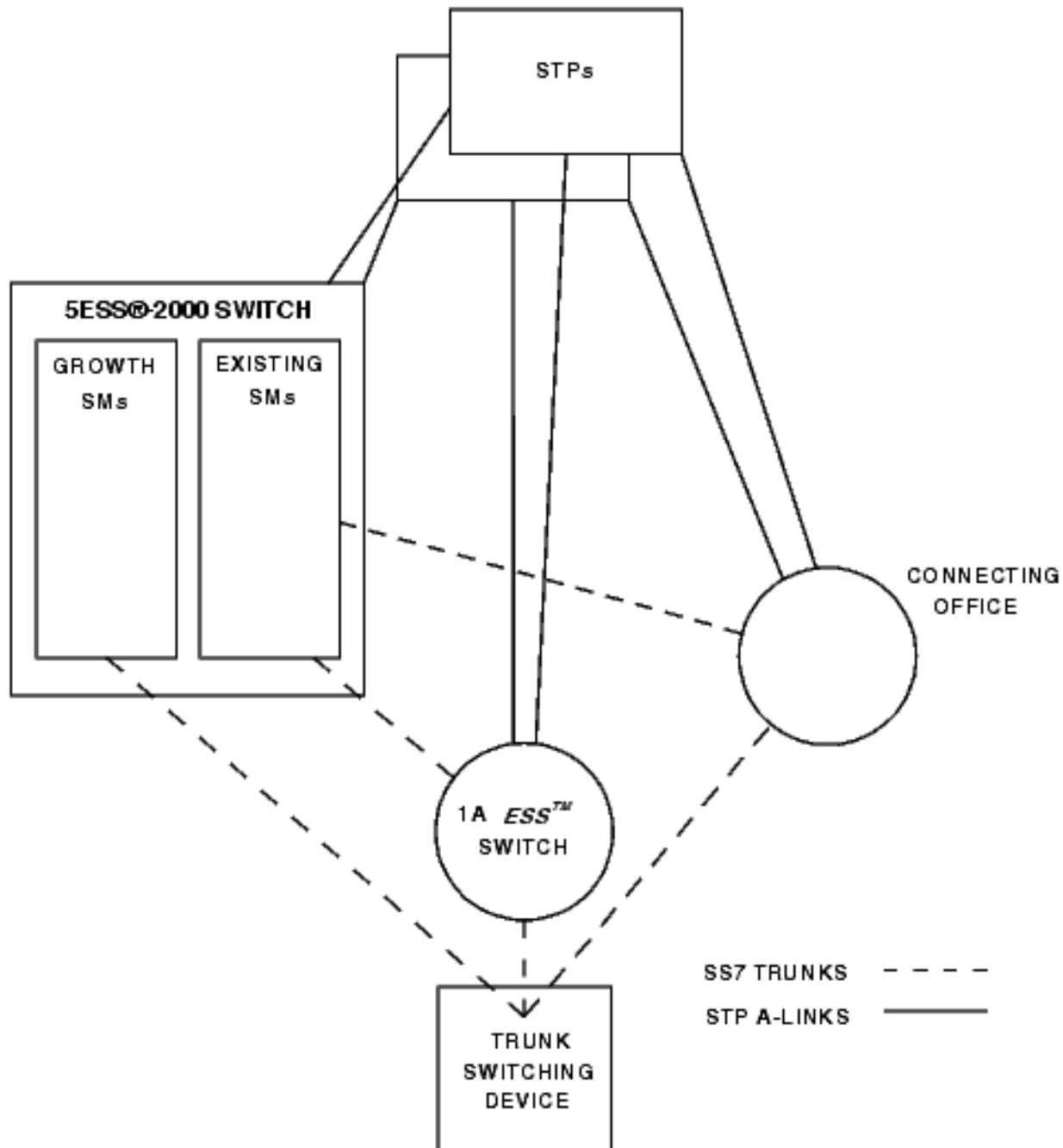


Figure 6-3 Flash Cut of Lines

6.5.4.2 Trunk Testing (Capped Switch)

The existing trunks in the 1A ESS™ switch can be reused and tested under the following conditions:

- (1) The 1A ESS™ switch trunks that are to be migrated to the 5ESS®-2000 switch after the retirement are segregated in new trunk groups in growth SMs. The reasons for segregating those to be reused was explained in the previous section. The originating point code (OPC) of the 5ESS®-2000 switch trunk groups to be tested contain 1A ESS™ switch point code (RC/V View 5.1, field ORIG PT CODE). Trunk groups to be

tested are set to emulate 2-wire switch (RC/V View 5.1, field VPA TYPE).

CAUTION: The 1A ESSTM switch trunk circuit identification code (TCIC) digits are not duplicates of the existing 5ESS[®]-2000 switch TCIC digits (RC/V View 5.1, field CLCI Code TRUNK ID). The reasons for this are detailed in the previous section.

- (2) The 5ESS[®]-2000 switch trunks to be tested must be in the out-of-service maintenance state CADN. The trunks must remain in the OOS CADN state until the 1A ESSTM switch is retired.
- (3) The 1A ESSTM switch TCIC information is duplicated in 5ESS[®]-2000 switch trunk information (RC/V View 5.5, field CLCI Code TRUNK ID).

6.5.4.3 Trunk Testing

- (1) Verify that trunk preconditions are met.
- (2) In the 1A ESSTM switch, populate the "pseudo" point code with the capping 5ESS[®]-2000 switch point code (RC:POINTC).
- (3) In the 1A ESSTM switch and the 5ESS[®]-2000 switch, activate the pseudo-point code capability (PPCC) feature (see "Turning the Feature On and Off," Section 6.5.5.7).
- (4) Perform Steps 2 through 10 of "Testing Existing Trunking," Section 6.5.6.2.
- (5) In the 1A ESSTM switch and the 5ESS[®]-2000 switch, turn off the PPCC feature (see "Turning the Feature On and Off," Section 6.5.5.7).
- (6) Verify that the 5ESS[®]-2000 switch trunks under test remain in the OOS CADN state.

6.5.4.4 Preretirement Conditioning

New or additional SMs are required in the 5ESS[®]-2000 switch to handle the additional lines and trunks when the 1A ESSTM switch is retired. The SMs can be thought of as growth out-of-service SMs. The growth trunking for the 5ESS[®]-2000 switch (that is, 1A ESSTM switch trunks) is assigned to the new growth SMs using new trunk groups and the 1A ESSTM switch circuit identification code assignments. The trunks will have their **VPA TYPE** in Recent Change View 5.1 set to emulate a 2-wire switch in the SMs. The existing trunk groups should not be used since PCCP will change the point code on a per SM basis.

In the connecting offices, the routes to the 5ESS[®]-2000 switch will have the next route index set to the trunk group connecting to the 1A ESSTM switch. This allows for route advancing through the 1A ESSTM switch if the route to the 5ESS[®]-2000 switch is busy.

When the 1A ESSTM switch is retired, the global title translations (GTT) in the STPs must be changed to allow TCAP messages that were completing to the 5ESS[®]-2000 switch point code to complete to the 1A ESSTM switch point code (that is, all TCAP messages completing to the 5ESS[®]-2000 switch that has assumed the 1A ESSTM switch point code). Sometimes, it may take time to make the GTT changes in the STPs, then TCAP queries would be lost during this time. Prior to switch retirement, one STP can be removed from service and the GTT changes are made. As part of the switch retirement, the STP with the updated GTT can be restored to service and the other STP can be removed from service to have its GTT updated. This avoids long periods when TCAP is unavailable.

6.5.4.5 Switch Replacement

The following procedures are used for the switch replacement:

- (1) In the growth SMs, use the PCCP to change the point code in the 5ESS[®]-2000 switch to the 1A ESSTM switch [which requires 3 to 5 minutes per switching module (SM)]. If pseudo-point code was used for trunk testing, the originating point code should be correct in the growth trunks, and this step is not required.
- (2) Remove the A-links from the 5ESS[®]-2000 switch. The switch goes into signaling point isolation (SPI) and the status of the connecting offices status is *transfer prohibited*. This causes all traffic to the 5ESS[®]-2000 switch point code to route through the 1A ESSTM switch point code.
- (3) In the 5ESS[®]-2000 switch, use Recent Change View 15.1 to change the **LOCAL POINT CODE** field of the CNI ring to the point code of the 1A ESSTM switch. The 5ESS[®]-2000 switch has assumed the point code of the 1A ESSTM switch.
- (4) Place the growth SMs in service.
- (5) In the 1A ESSTM switch, remove the A-links and connect them to the 5ESS[®]-2000 switch. When the links prove-in (go active), the 5ESS[®]-2000 switch becomes the 1A ESSTM switch point code to the network.
- (6) Move the trunks from the 1A ESSTM switch to the 5ESS[®]-2000 switch. All traffic to both point codes is passed through the 1A ESSTM switch trunks.

NOTE: It should be noted that prior to moving the links to the new switch the links should *not* be removed from service (MOOS). If the first link is removed from service and moved to the new switch, it cannot be restored to service until the second link is moved to the new switch. When the first link is moved to the 5ESS[®]-2000 switch in an out-of-service (OOS) state and then requested to be put in service from the 5ESS[®]-2000 switch, the STP will use the in service (IS) link to poll the switch. The IS link is still attached to the 1A ESSTM switch and the status of the other link on the 1A ESSTM switch is OOS.

- (7) Perform the line cutover.
- (8) In the STPs, restore to service the STP with the updated GTTs and remove from service the other STP to update the GTTs. The STP should be restored to service as soon as the GTTs are updated.
- (9) In the 5ESS[®]-2000 switch, remove from service the trunk groups (OOS-CADN) in the existing SMs that were associated with the previous point code.
- (10) Use the PCCP to change the point codes in the administrative module (AM) and SMs for the trunk groups that were associated with the previous point code. (This requires 3 to 5 minutes per SM.)
- (11) In the connecting offices, change the point code of the trunk groups associated with the previous 5ESS[®]-2000 switch point code to the new 5ESS[®]-2000 switch point code. Since the point code has been changed, glare treatment must be verified to ensure that it is proper.
- (12) Place the trunk groups in service.
- (13) Run trunk query audits to verify that all SS7 trunks are in the same state. The methods are as follows:
 - At the 5ESS[®]-2000 switch:
AUD; CCSTQ, TKGMN=xxx-y

NOTE: This message will process 16 circuit identification codes at a time.

- At the 4ESSTM switch:
TEST:TRUNK, CIN 1001THISISACIN116T;TQU!
- At the 1A ESSTM switch:

TQ-TNN-	(individual trunk)
TQ-GROUP-	(trunk group)
TQ-DPC-	(all trunks in groups to destination point code)
TQ-ALL-	(whole office)

(14) Retirement is completed.

6.5.4.6 Post-Retirement Cleanup

After retirement, cleanup effort is required.

In the STPs, remove the point code associated with the previous 5ESS[®]-2000 switch point code. Change the CLLI code to the 5ESS[®]-2000 switch for the new 5ESS[®]-2000 switch point code (that is, 1A ESSTM switch point code).

Some types of offices store the far-end CLLI code and use them for manually requested (information only) diagnostics. The 4ESSTM switch and 5ESS[®]-2000 switch store the far-end CLLI code and use this information to run manually requested TIC, CVT, and XLATE tests. This information must be changed in connecting offices before the tests can be run. The forms/views that can be used to make changes in populated SS7 groups are as follows:

- 5ESS[®]-2000 switch (Recent Change, View 5.1)
- In the 4ESSTM switch a CLLI code cannot be duplicated in the switch. The CLLI code "far sub-building" can be changed in a populated TSG. To verify that the new CLLI code does not exist in the 4ESSTM switch a VER:TFNB:TG tname! must be used. If the CLLI code does not exist, the Recent Change Form 802 can be used to change the CLLI code. If the CLLI code currently exists it must be removed before attempting any changes via the RC form 802.

The trunk groups that were moved to the new switch from the 1A ESSTM switch are operating with a **VPA TYPE** of 2-wire emulation on the 5ESS[®]-2000 switch. These should be changed to the 4-wire mode. (See "Changing VPA Type After Cutover," Section 6.5.6.10 for details.)

6.5.5 Using The Existing Point Code On The Replacing Switch

6.5.5.1 Special Procedure for Reusing Point Codes

If the 1A ESSTM switch point code is reused in the new switch, a special procedure is required during trunk testing and cutover. This procedure avoids additional work in the connecting offices and replacing switch. To use this procedure, the circuit identification code information in the 1A ESSTM switch must be used to populate the 5ESS[®]-2000 switch ODD. This is required since all the connecting offices contain the circuit identification code information. Any additional trunking for the new facility must be kept in the out-of-service state until after switch replacement. For trunk testing of reused and growth trunks, the **PSEUDO-POINT CODE CAPABILITY** must be loaded in both the retiring 1A ESSTM and replacing 5ESS[®]-2000 switch, respectively.

6.5.5.2 Pseudo-Point Code Capability Feature Description

The pseudo-point code allows for the testing of SS7 trunks without having to use a temporary point code to identify

the installing 5ESS®-2000 switch in the connecting offices. During this test interval, temporary A-links will be required from the STP to the installing 5ESS®-2000 switch. After trunk testing is completed, the A-links should be removed. The A-links to the old switch should be moved to the new switch as part of the cutover procedure. This prevents making changes in the STP during the cutover. Figure 6-4 illustrates the configuration of the offices during trunk testing. To simplify the diagram, only one mated STP pair is shown.

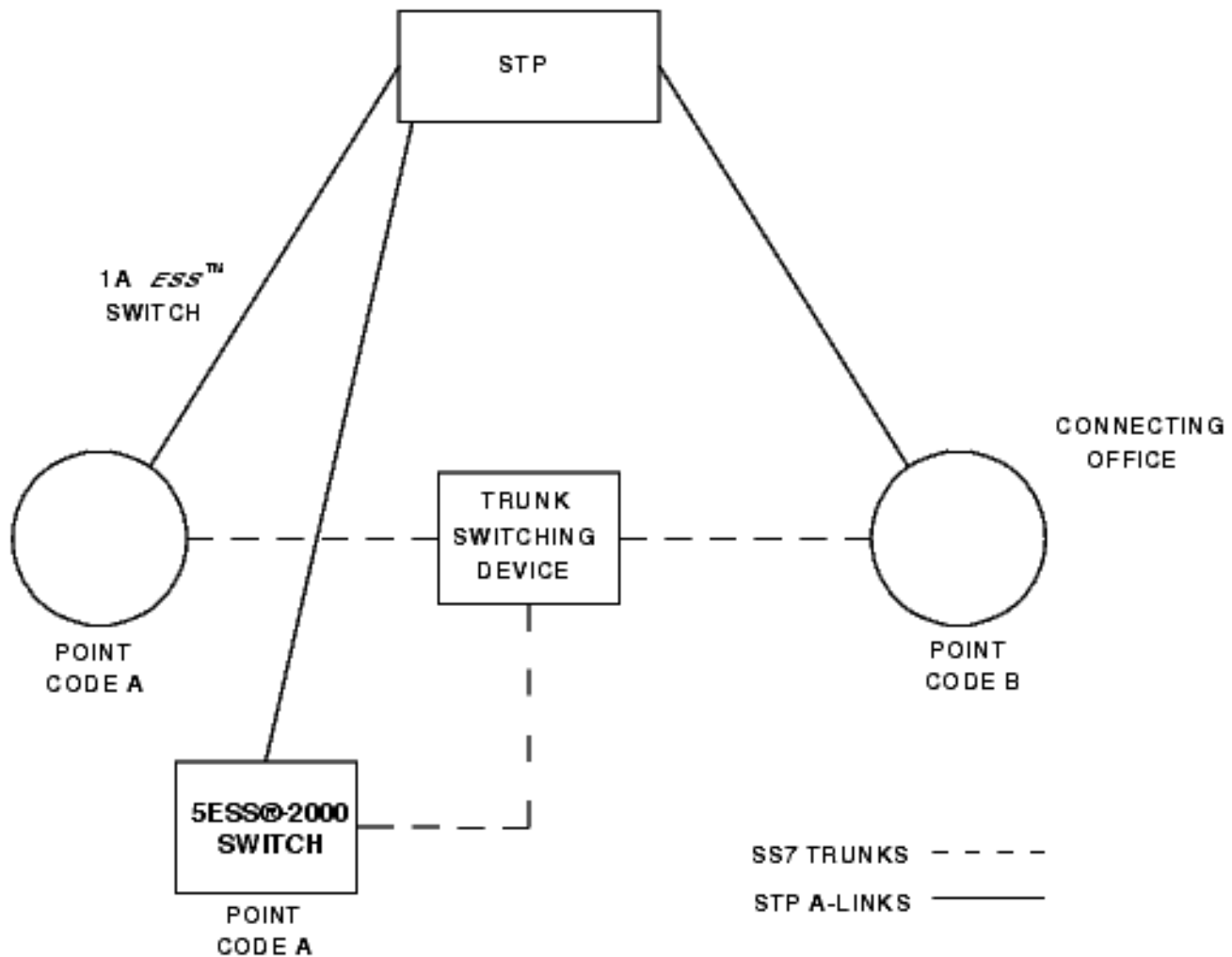


Figure 6-4 SS7 Trunk Testing Configuration

During the trunk test interval, a Special Maintenance state is used in the 1A ESS™ switch for trunks that are being reused in the replacing switch. This state indicates that (1) the trunk under test is actually connected to the 5ESS®-2000 switch, (2) all normal SS7 messages for the trunk under test are redirected to the 5ESS®-2000 switch, and (3) certain maintenance messages will be handled by the 1A ESS™ switch. For growth trunks that do not appear at the 1A ESS™ switch, the 1A ESS™ switch will redirect all SS7 messages to the 5ESS®-2000 switch.

6.5.5.3 5ESS®-2000 Switch Features

The primary method for verifying the continuity of an SS7 trunk is the voice path assurance test. Depending on the type of connecting office (that is, 2-wire or 4-wire), a different set of frequencies is used to verify the talking path. This test is done as part of the normal call setup on a sampling or 100 percent basis. The 1A ESS™ switch is a 2-wire switch and the 5ESS®-2000 switch is a 4-wire switch. This switch type information is stored in all the

connecting offices. The 5ESS®-2000 switch is capable of emulating a 2-wire switch for the purposes of voice path assurance testing. The 2-wire emulation values are assigned on a per-trunk group basis (Recent Change View 5.1 field **VPA TYPE**) in the 5ESS®-2000 switch. The 2-wire emulation should be used during trunk testing and during cutover to avoid making changes in all the connecting offices. The enumerations for 2-wire emulation are 2W4WL[0-3] and 2W2WL[3-5]. The first number is the local switch type (a 2 will be used for 2-wire emulation). The second number is the type of connecting offices (that is, 2-wire or 4-wire). The last numbers are the decibel loss.

6.5.5.4 1A ESS™ Switch Features

The 1A ESS™ switch pseudo-point code capability is feature group **9SPGCC** and is available in the 1AE10.08 and 1AE11.02 and later software releases. Ordering information can be found in the 1A Central Office Equipment Engineering System (1A COEES) manual.

6.5.5.5 Trunk Testing Using the Existing Point Code on the Replacement Switch

For trunk testing to be performed without making changes in the connecting offices, the trunk groups to be tested in the 5ESS®-2000 switch must have **VPA TYPE** set as 2-wire emulation (Recent Change View 5.1). The circuit identification code information must be the same in both the 1A ESS™ switch and the 5ESS®-2000 switch. The 5ESS®-2000 switch must also be in the pre-cut state and all SS7 trunks should be **OOS CADN**. Since the trunks are in a special maintenance state on the 1A ESS™ switch during trunk testing, the trunk query audit must be turned off in the 5ESS®-2000 switch (Recent Change View 5.1 TRK QUERY = N) during trunk testing.

6.5.5.6 Populating the Temporary Point Code

In the 1A ESS™ switch, use RC message `RC:POINTC:PSPC` to populate the pseudo-point code feature with the temporary point code of the 5ESS®-2000 switch.

In the 5ESS®-2000 switch, use Recent Change View 15.1, field `LOCAL POINT CODE`, to populate the CN1 ring with the temporary point code. Cluster routing must exist for the cluster where the 1A ESS™ switch (to be replaced) resides.

6.5.5.7 Turning the Feature On and Off

In the 1A ESS™ switch, the feature can be activated by the teletypewriter (TTY) message `ALW:PROGCTRL PPC` and inhibited by the message `INH:PROGCTRL PPC`.

In the 5ESS®-2000 switch, the feature can be activated by using ODBE with the following input values:

- Processor: AM
- Relation: PARAMETER
- Parameter name: GL1ARPL=DBYES.

The pseudo-point code capability is fully activated by a combination of data conditions: Recent Change View 15.1, **LOCAL POINT CODE**, is not equal to the OPC in trunk data View 5.1 and the parameter GL1ARPL=DBYES. The feature can be deactivated by setting the parameter GL1ARPL=DBNO and changing the point code in Recent Change View 15.1 to agree with the trunk data. After the ODBE change, a system audit must run to update office parameters. The audit can take up to 15 minutes to run.

6.5.5.8 5ESS®-2000 Switch Call Route Testing

When the PPC is active test calls can be placed from the 5ESS[®]-2000 switch to verify call routing. This can be done for trunks that are in the Special Maintenance state on the 1A ESSTM switch, connected to the 5ESS[®]-2000 switch and PPC active on both switches. During trunk testing the trunks to be tested are kept in the OOS CADN state. After the trunk has been tested the routing of outgoing and two-way trunks to the connecting office can be tested using test phones in the 5ESS[®]-2000 switch.

The trunk under test is first placed In Service (IS) on the 5ESS[®]-2000 switch. The 5ESS[®]-2000 switch will send a request message to the 1A ESSTM switch to place the trunk in service. The 1A ESSTM switch will send a response message to the 5ESS[®]-2000 switch. Since the trunk under test is in the Special Maintenance state in the 1A ESSTM switch the 1A ESSTM switch will not restore the trunk to service nor pass the restore message to the connecting office. At this point the trunk is in service on the 5ESS[®]-2000 switch, out of service SM on the 1A ESSTM switch and out of service in the connecting office.

A test phone in the 5ESS[®]-2000 switch can now be used to originate a call to the connecting office. The outgoing trunk routing can be tested. The SS7 messages will be redirected through the 1A ESSTM switch to the connecting office. The trunk under test will be used to complete the call. Since the trunk is out of service in the connecting office the trunk in the connecting office will not be placed in service after the test call is abandoned. Also since the trunk is out of service in the connecting office test calls cannot be originated in the connecting office from a test phone.

After the routing has been verified the trunk under test in the 5ESS[®]-2000 switch must be placed in the OOS CADN state. The 5ESS[®]-2000 switch will send a request to the 1A ESSTM switch. The 1A ESSTM switch will respond to the 5ESS[®]-2000 switch but not change the Special Maintenance state of the trunk or pass the request to the connecting office.

6.5.6 Normal Replacement (Non-CAP)

6.5.6.1 Pre-Trunk Test Conditions

CAUTION: Before the replacing 5ESS[®]-2000 switch "A" links are connected to the STP, the following conditions must be met:

- (1) The 5ESS[®]-2000 switch temporary "pseudo" point code must be populated in the STP.
- (2) The 5ESS[®]-2000 switch must have cluster routing information (RC/V View 15.9) to the 1A ESSTM switch. The 1A ESSTM switch must have cluster routing (function ROUTE) to the 5ESS[®]-2000 switch.
- (3) The trunk groups to be tested in the 5ESS[®]-2000 switch must be set to emulate a 2-wire switch (RC/V View 5.1, field VPA TYPE). The trunk groups to be tested are populated with the 1A ESSTM switch point code (RC/V 5.1, field ORIG PT CODE). The 5ESS[®]-2000 switch trunks to be tested are populated with 1A ESSTM TCIC data (RC/V 5.5, field CLCI Code TRUNK ID).
- (4) The trunks in the 5ESS[®]-2000 switch must be placed in out-of-service maintenance state "CADN" (RMV:TRK, TKGMN). With the trunks in the CADN state, the trunk group query audit must be disabled (RC/V View 5.1, field TRK QUERY=N).
- (5) The 5ESS[®]-2000 switch (RC/V View 15.1 "LOCAL POINT CODE") must be populated with the temporary "pseudo" point code.
- (6) The 1A ESSTM switch must be populated with the temporary "pseudo" point code (RC:POINTC).
- (7) The pseudo-point code feature must be active in both retiring 1A ESSTM switch and the replacing 5ESS[®]-2000 switch. See "Turning the Feature On and Off," Section 6.5.5.7.

These steps are required to prevent the precut 5ESS[®]-2000 switch from sending any messages to other nodes in the SS7 network. With the feature active and populated with the proper point codes, all 5ESS[®]-2000 switch messages will be sent to the 1A ESSTM switch. The 1A ESSTM switch will decide on the proper disposition of the message. The feature should be left enabled during the entire test interval.

6.5.6.2 Testing Existing Trunking

The following steps should be followed for testing trunks that are reused in the replacing office using the pseudo-point code capability:

- (1) Verify that all of the pre-trunk testing conditions ("Pre-Trunk Test Conditions," Section 6.5.6.1) are met.
- (2) In the 1A ESSTM switch, place the trunks to be tested in the out-of-service BUSY state, T-TNN-MB 0 0 XXXXXX. This causes the state of the trunks in the connecting office to go to the out-of-service remotely blocked state.
- (3) Move trunk facilities to be tested to the 5ESS[®]-2000 switch. Trunk wiring is now connected from the connecting office to the 5ESS[®]-2000 switch. Refer to Figure 6-4 for an illustration of trunk wiring.
- (4) In the 1A ESSTM switch, place the trunks to be tested in the special maintenance state, T-TNN-SM 00 XXXXXX. This activates pseudo-point code on these trunks. The trunks in the special maintenance state can be verified by the input message, T-TNN-RS 00 XXXXXX. The trunks will be in the Special Maintenance state.
- (5) Test trunks using local procedures.
- (6) Fix any failing trunks.
- (7) In the 1A ESSTM switch, move the trunks under test back to the out-of-service state, T-TNN-SO 00 XXXXXX. This deactivates pseudo -point code for that trunk.
- (8) Move trunk facilities back to the 1A ESSTM switch. Trunk wiring is now connected from the connecting office to the 1A ESSTM switch.
- (9) In the 1A ESSTM switch, place the trunks in service, T-TNN-MA 0 0 XXXXXX. The trunks in the connecting office should be in the IN SERVICE STATE.
- (10) From the connecting office, request the trunk query audit and verify the trunks are in a consistent state. The methods are as follows:

- At the 1A ESSTM switch:

TQ-TNN-	(individual trunk)
TQ-GROUP-	(trunk group)
TQ-DPC-	(all trunks in groups to destination point code)
TQ-ALL-	(whole office)

- At the 5ESS[®]-2000 switch:
AUD; CCSTQ, TKGMN=xxx-y
- At the 4ESSTM switch:
TEST:TRUNK, CIN 1001THISISACIN116T;TQU!

- (11) During the test interval the pseudo-point code feature should be left enabled. This will force all messages form the precut 5ESS[®]-2000 switch.
- (12) Repeat Steps 1 through 11 until all the trunks are tested.

6.5.6.3 Testing New or Growth Trunks

The following procedure should be used to test trunks that are being added to the replacement office, but do not appear in the office being replaced. If the trunk under test is to an office whose point code is not defined in the 1A ESSTM switch, the point code of the connecting office must be defined in the 1A ESSTM switch using the RC:POINTC:PC message. This is required to allow the 1A ESSTM switch to redirect the messages to the 5ESS[®]-2000 switch.

- (1) Verify that all pre-trunk testing conditions are met.
- (2) In the connecting office and the 5ESS[®]-2000 switch, the trunks should be out of service (OOS CADN in the 5ESS[®]-2000 switch) with the connecting office being locally blocked.
- (3) Test the trunks using local procedures and repair as necessary.
- (4) During the test interval, the pseudo-point code feature should be enabled. This will force all messages form the precut 5ESS[®]-2000 switch.

6.5.6.4 Precutover Procedure

When trunk testing is completed, the pseudo-point code feature must be deactivated and the temporary point code and signaling link (SLK) information must be removed from the STPs.

NOTE: **HOME** and **MATE** are software release terms for the local 2/ASN STPs. The customer will determine which STP is assigned as **HOME** or **MATE**.

6.5.6.5 Isolating the 5ESS[®]-2000 Switch

At the 5ESS[®]-2000 switch, disconnect the **HOME** and **MATE** signaling links by unplugging the A-links from the data sets. The 5ESS[®]-2000 switch will go into signaling point isolation.

Verify that the pseudo-point code feature is deactivated in both switches (see "Turning the Feature On and Off," Section 6.5.5.7 for more details).

Place the permanent point code in the 5ESS[®]-2000 switch common network interface (CNI) ring (Recent Change View 15.1, field **LOCAL POINT CODE**).

At the **HOME** and **MATE** STPs, degrow the link nodes associated with the 5ESS[®]-2000 switch temporary signaling links. This prevents any messages from printing at the STP about link outage.

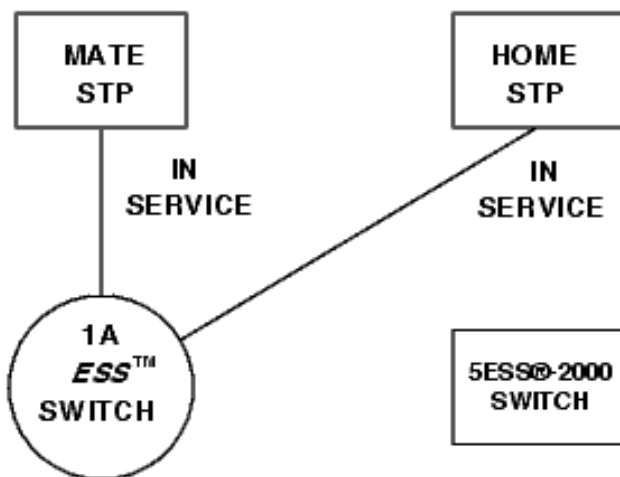
Verify the cluster routing in the 5ESS[®]-2000 switch by use of the input message OP:C7NET,PRTE. This is required since only cluster routing to the 1A ESSTM switch being replaced was used during testing. The routing must be identical to the 1A ESSTM switch except all routing will be blocked. Verify that the signaling link code (SLC) information on the Recent Change View 15.2 agrees with the 1A ESSTM switch information. Verify that the subsystem information for Local Area Signaling Service (LASS) and service switching point (SSP) (Recent Change Views 8.17, and 15.10) agree with the 1A ESSTM information.

6.5.6.6 Testing the Permanent STP Links

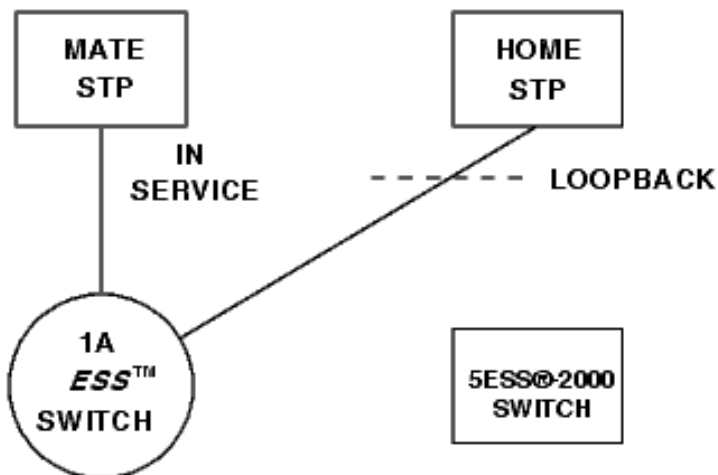
The signaling links should be tested before cutover to prove that a good physical connection exists between the STPs and the 5ESS[®]-2000 switch. The testing should be done during low traffic period (since an A-link is removed from the existing 1A ESSTM switch and moved to the new 5ESS[®]-2000 switch). The same procedure should be used during the cutover via the use of cutover devices, or by moving the link at the switch distribution panel. During the following procedure, the 5ESS[®]-2000 switch will not be allowed to go into service.

- (1) At the 5ESS[®]-2000 switch, turn on the signaling link monitor (MON:SLK. . .).
- (2) At the **HOME** STP, activate local and digital loopback at the signaling links data set (Figure 6-5). In this position, all signals received from the 5ESS[®]-2000 switch will be looped back to the switch.
 - For the Lucent Technologies 2500 series, press the digital loopback (DL) button.
 - For DATATEL[®] 3180 series, press the local digital loopback (LDL) button.
 - For all other data sets, the operating manual should be consulted.
- (3) At the 1A ESSTM switch, disconnect the **HOME** STP signaling link and connect it to the 5ESS[®]-2000 switch. At this point, all signaling from the 5ESS[®]-2000 switch to the **HOME** STP is being returned. Since the 5ESS[®]-2000 switch is signaling point isolation, an emergency prove-in on the link will be started.
- (4) The signaling link will pass prove-in levels 1 and 2, but will fail level 3 because of the digital loopback at the **HOME** STP office. The signaling link test (SLT) acknowledgment failure will be seen at the 5ESS[®]-2000 switch (Figure 6-6). This shows connections from the 5ESS[®]-2000 switch to the **HOME** STP signaling link data set pass successfully.
- (5) At the 5ESS[®]-2000 switch, disconnect the **HOME** STP signaling link and reconnect it to the 1A ESSTM switch.
- (6) At the **HOME** STP data set, remove the loopbacks and verify that the link proves in and the link is returned to service.
- (7) At the 5ESS[®]-2000 switch, remove the signaling link monitor (MON:SLK=. . . :OFF).
- (8) The **MATE** STP should then be tested using the same procedure.

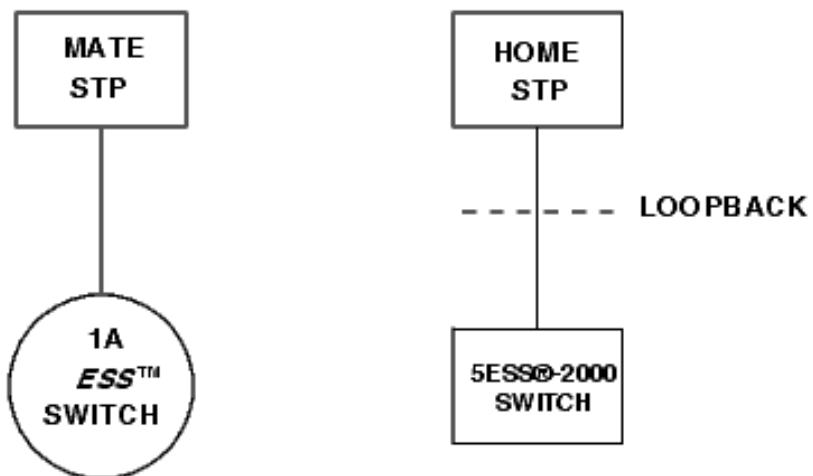
A. BEFORE TESTING



B. LOOPBACK DATA SET



C. MOVE LINK TO SWITCH



STP A-LINKS ———

Figure 6-5 Link Testing Procedures

S000-50 89-05-27 00:30:38 007493
REPT MON:SLK
SLK 32 03 NAPRVILB01W AVL OOS

RECEIVER LINK FAILURE, 2663568012

S000-50 89-05-27 00:30:40 007495
REPT MON:SLK
SLK 32 03 NAPRVILB01W AVL OOS

LEVEL 2 ACTIVE, 2663570021

S000-50 89-05-27 00:30:40 007496
REPT MON:SLK
SLK 32 03 NAPRVILB01W AVL OOS

LEVEL 3 ACTIVE RECOVERY STARTED,
2663570319

S000-50 89-05-27 00:30:40 007497
REPT MON:SLK
SLK 32 03 NAPRVILB01W AVL OOS

SS7 SLT, OPC=F648A1, DPC=F64700,

SLC=0 2663570319

S000-50 89-05-27 00:30:40 007498
REPT MON:SLK
SLK 32 03 NAPRVILB01W AVL OOS

SS7 SLT-NOT PACKED,
OPC NOT EQUAL FEPC,
2663570334

S000-50 89-05-27 00:30:41 007500
REPT MON:SLK
SLK 32 03 NAPRVILB01W AVL OOS

SS7 SLTA TIMER EXPIRED
2663571047

S000-50 89-05-27 00:30:41 007503
REPT MON:SLK
SLK 32 03 NAPRVILB01W AVL OOS

SS7 SLT, OPC=F648A1, DPC=F64700,
SLC=0 2663571334

S000-50 89-05-27 00:30:41 007504
REPT MON:SLK
SLK 32 03 NAPRVILB01W AVL OOS

SS7 SLT-NOT PACKED,

OPC NOT EQUAL FEPC,

2663571347

Figure 6-6 Link Testing Messages

6.5.6.7 Cutover Precedence

During an SS7 switch cutover, the three primary areas are line cutover, trunk cutover, and signaling link cutover. The 5ESS®-2000 switch line cutover procedure is located in 235-105-200, *Precutover and Cutover Procedures* manual. During the line cutover, the central office line connector in the 1A ESS™ switch will not be open until the customer goes on-hook. The trunk cutover involves moving existing trunking from the old switch to the new switch. It also involves the use of cutover devices or the movement of trunk cables. Calls on these trunks will be lost when the trunks are moved. The method used for line and trunk cutover depends on local procedures. The signaling link cutover involves moving of the signaling links from the old switch to the new switch. The exact order that these are performed in is governed by local procedures. A typical cutover procedure is given and emphasizes the moving of the signaling links. The procedure used for cutover does not require the line, trunk, and signaling link cutover be done in a specific order.

6.5.6.8 Switch Cutover

The procedures for switch cutover are as follows:

- (1) At the 5ESS®-2000 switch, verify that the SS7 trunks are either idle or in the periodic reset state.
- (2) At the ASN STPs, use Page 1141 to verify that the signaling links to the 1A ESS™ switch are active and stable. In the 1A ESS™ switch, use Page 1108 to verify the signaling links are active and stable. In the 5ESS®-2000 switch, use Page 118 to verify that both links are in the emergency restart state.
- (3) At each ASN STP and at the 5ESS®-2000 switch, turn on the signaling link monitor (MON:SLK= . . .).
- (4) At each ASN STP and at the 1A ESS™ switch, inhibit automatic removal of link nodes for diagnostics on declared failures (INH:RMV:ON).
- (5) At the **HOME** ASN STP, activate loopback on the data set for the 1A ESS™ switch signaling link (see "Testing the Permanent STP Links," Section 6.5.6.6, for more details).
- (6) At the 1A ESS™ switch, disconnect the **HOME** ASN STP signaling link and connect it to the 5ESS®-2000 switch. The link will pass level 1 and level 2 prove-in, but will fail level 3 signaling link test acknowledgment (Figure 6-6). The link is ready for cutover.

NOTE: It should be noted that prior to moving the links to the new switch, the links should **not** be removed from service (MOOS). If the first link is removed from service and moved to the new switch, it cannot be restored to service until the second link is moved to the new switch. When the first link is moved to the 5ESS®-2000 switch in an out-of-service (OOS) state and then requested to be put in service from the 5ESS®-2000 switch, the STP will use the in service (IS) link to poll the switch. The IS link is still attached to the 1A ESS™ switch and the status of the other link on the 1A ESS™ switch is OOS.

- (7) At the **HOME** ASN STP, remove loopback from the signaling link data set. The link will prove in within 5 seconds. If the link does not prove in, check the data sets on each end of the signaling link for send and receive data indications. If the link does not prove in, the cutover should be stopped until the link can be proved in. The STP is now sending messages to both switches so the next step must be done as quickly as possible.
- (8) At the 1A ESS™ switch, remove the **MATE** STP signaling link and connect it to the 5ESS®-2000 switch. The link starts to prove in and goes in service within 30 seconds. The 1A ESS™ switch goes into signal point

isolation. The 5ESS®-2000 switch is now receiving all SS7 messages.

- (9) Start the line cutover from the 1A ESS™ switch to the 5ESS®-2000 switch.
- (10) Start the trunk cutover from the 1A ESS™ switch to the 5ESS®-2000 switch.
- (11) At each ASN STP and the 5ESS®-2000 switch, allow automatic removal of the link nodes for diagnostics on declared failure (ALW:RMV:ON).
- (12) At each ASN STP and the 5ESS®-2000 switch, turn off the monitor of the signaling links (MON:SLK=...:OFF).
- (13) When the trunk cutover is completed, the state of the trunks should be consistent in both the new switch and the connecting offices. To verify this, the trunk query audit should be run in both the new switch and the connecting offices. This audit is run automatically once a day or via request.

To manually request the audit, the following messages should be used:

- At the 5ESS®-2000 switch:
AUD; CCSTQ, TKGMN=xxx-y

NOTE: This message will process 16 circuit identification codes at a time. The CCSTQ audit is scheduled by a time value of when to start each group of 16 trunks on View 8.15. The timer can be reduced to a minimum to allow all trunks to be tested in the shortest amount of time.

- At the 1A ESS™ switch:

TQ-TNN-	(individual trunk)
TQ-GROUP-	(trunk group)
TQ-DPC-	(all trunks in groups to destination point code)
TQ-ALL-	(whole office)

- At the 4ESS™ switch:
TEST:TRUNK, CIN 1001THISISACIN116T;TQU!

- (14) Cutback operations.

This section should only be performed for unexpected SS7 signaling failures to the 5ESS®-2000 switch or unexpected trunk failures to/from the 5ESS®-2000 switch.

In the event of massive signaling failures, disconnect the signaling links from the 5ESS®-2000 switch and reconnect them to the corresponding positions in the 1A ESS™ switch. Verify that the signaling links go from emergency restart state to activate state.

Check data sets, facilities, and link data between the 5ESS®-2000 switch and **HOME** and **MATE** ASN STPs to ensure correct settings, connections, and data.

Start converting lines and trunks back to the 1A ESS™ switch.

6.5.6.9 Post-Cutover Procedure

When the switch replacement is completed and the new switch appears stable, the link nodes at the 1A ESS™ switch can be degrown.

With a new switch, the CLLI code for the new office may be different from the old switch. The 4ESSTM switch and 5ESS[®]-2000 switch store the far-end CLLI code and use this information to run manually requested `TIC`, `CVT`, and `XLATE` tests. This information must be changed in connecting offices before the tests can be run. The forms/views that can be used to make changes in populated SS7 groups are as follows:

- 5ESS[®]-2000 switch (Recent Change, View 5.1)
- In the 4ESSTM switch a CLLI code cannot be duplicated in the switch. The CLLI code "far sub-building" can be changed in a populated TSG. To verify that the new CLLI code does not exist in the 4ESSTM switch a `VER:TFNB:TG tname!` must be used. If the CLLI code does not exist, the Recent Change Form 802 can be used to change the CLLI code. If the CLLI code currently exists it must be removed before attempting any changes via the RC form 802.

The ASN STPs store the switch CLLI codes and must be changed. This can only be done by degrowing the link; therefore, it should be done during a period of light traffic. The following procedures should be done serially at each ASN STP:

- (1) Remove the link from service (`CHG:SLK=...:MOOS`). Service from the STP to the 5ESS[®]-2000 switch will be lost and all SS7 traffic will be via the other STP.
- (2) If GTT routing is done at the STP, delete any GTT routing data to the 5ESS[®]-2000 switch point code (Data Management System function `ordgntt`).
- (3) Delete ordered route data for the signaling links set (Data Management System function `ordrte`).
- (4) Move the signaling link to the `UAV` state (Data Management System function `lnkdat`).
- (5) Move the link set point code and CLLI code to an unassigned point code (in the same network) and unassign the CLLI code (Data Management System function `lnkset`). The ASN STP requires that if the CLLI code is changed, the point code must also be changed. Both must be set to unassigned values so that in the next step, both can be changed back to those of the 5ESS[®]-2000 switch.
- (6) Change the link set point code and CLLI code to the 5ESS[®]-2000 switch point code and CLLI code (Data Management System function `lnkset`).
- (7) Put back the ordered route data deleted in Step 3 (Data Management System function `ordrte`).
- (8) If any GTT routing data was deleted in Step 2, put it back (Data Management System function `ordgntt`).
- (9) Change the signaling link state back to out of service (Data Management System function `lnkdat`).
- (10) Restore the signaling link to service (`CHG:SLK=...:IS`).

6.5.6.10 Changing VPA Type After Cutover

After switch replacement, the new switch is emulating a 2-wire switch for VPA testing. It is advisable to change the VPA to reflect that the new switch is a 4-wire switch. The reason for this is to avoid confusion in isolating problems after switch replacement. The VPA tests for 2-wire and 4-wire switches are different and require changes in both the new switch and the connecting office.

6.5.6.10.1 5ESS[®]-2000 Switch

In the 5ESS[®]-2000 switch, the VPA type is located in Trunk Group (RC View 5.1). This value can be changed in an active trunk group. The VPA type in the new 5ESS[®]-2000 switch will be either 2W4WL[0-3] or 2W2WL[3-5]. The convention for VPA is the first digit is for the local switch and the second digit is for the far end switch. Since the 5ESS[®]-2000 switch was emulating a 2-wire switch for VPA, the first digit will be a 2.

If the connecting office is a 5ESS[®]-2000 switch, the VPA should be changed to 4W4WL[0-3] in both switches.

6.5.6.10.2 1A ESSTM Switch

In the 1A ESSTM switch, the type of connecting office is located in bit 14 of the first word of the Trunk Class Code (TCC). The TCC is a common item and is usually shared among several TG's. In the 1A ESSTM switch, a TG can contain more than one circuit type so the TCC is not stored on a TG but on a TNN basis.

One method of changing the type of connecting office in the 1A ESSTM switch is to create a new TCC in the 1A ESSTM switch for the TG going to the switch that is being replaced. It should initially be populated with the type of connecting office as a 2-wire switch. After the switch is replaced and the VPA is to be changed, RC:PSWD can be used to change the type of connecting office.

If a new separate TCC cannot be created and an existing TCC must be used, a new TG can be created and the trunks in the old TG can be degrown and moved to the new TG to update the TCC.

An alternative to rolling the trunks into a new TG is to use RC:PSWD to change the TCC on a per-TNN basis. The TCC for the trunk is stored in the TNN to TGN translator. A TAG-TNN message can be used to find the start of the translator and RC:PSWD can be used to change the TCC. A library program could be used to automate this process.

If the previous system is used, the trunks can be left in service while the changes are made under the following conditions. The VPA rate in the 5ESS[®]-2000 switch must be set to 0 (RC 5.1)

When the 1A ESSTM switch originates the VPA test to either a 2-wire or 4-wire switch, it always transmits at a frequency of 2010 Hz and expects to receive at 1780 Hz. When a 4-wire switch originates a VPA test to a 2-wire switch, the 4-wire switch transmits at 1780 Hz and expects to receive 2010 Hz. Figure 6-7 illustrates these exchanges. After the changes to the TCC have been made to the 1A ESSTM switch, the VPA type can be changed in the 5ESS[®]-2000 switch and the VPA rate changed.

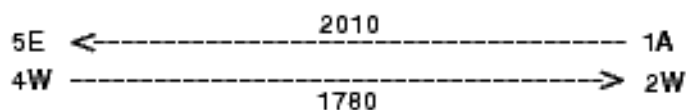
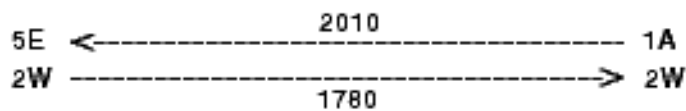


Figure 6-7 VPA Test Exchanges**6.5.6.10.3 4ESSTM Switch**

In the 4ESSTM switch, the VPA type is stored on a Trunk Subgroup (TSG) basis and cannot be changed using the RC:TSG message. This value cannot be changed in a populated TSG.

7. TRUNK CONVERSION

This section contains information for converting per-trunk signaling (PTS) trunks to the Signaling System 7 (SS7) protocol. Items to be done prior to manual conversion are covered in "Manual Preconversion Requirements," Section 7.1. Procedures for manual conversion are covered in "Manual Trunk Conversion Procedures," Section 7.2. Finally, automated protocol conversion using the Enhancements for Simultaneous Trunk Conversion via Automatic Recent Change (STAR) is covered in "Automated Trunk Conversion," Section 7.3.

7.1 MANUAL PRECONVERSION REQUIREMENTS

7.1.1 Procedures

When performing trunk conversion procedures, the following items must be completed:

- (1) The common network interface (CNI) ring and signaling links to the signaling transfer points (STPs) in the common channel signaling (CCS) network are operational and all tests have passed.
- (2) The STP has been updated with the point codes and other data relating to the offices between which the trunks are connected.

NOTE: Point codes should be assigned 1-to-1 with NEAR CLLI code values. Trunks homed on remote switching modules (RSMs) are given the same point code as those trunks homed on any other switching modules
- (3) Any switching module on which CCS trunks [ISDN User Part (ISUP)] terminate must be equipped with a Digital Service Unit Module 2 (DSU2).
- (4) All the Class 15 views in recent change that are needed have been populated, and the office related Views 8.1 and 8.15 are populated.
- (5) The far-end office of the trunks designated for conversion is in sync with the office making the conversion and the far-end office is performing the necessary conversion changes at the same time.

CAUTION: The far-end office must have all SS7 capabilities fully implemented and operational prior to any routing changes or trunk conversions.

- (6) Since the conversion is being done to trunks that are already in use, it is assumed that the trunk hardware has been tested, all tests passed, and trunks are operational.

7.1.2 Trunk Verification Tests

If the local exchange carrier (LEC) wishes to test the trunks with the far-end to verify their proper operation, the test trunk message may be used. With this input message, the user may request a transmission test or give a particular trunk a directory number to outpulse.

The following message may be used to test a trunk, a range of trunks, or a trunk group:

TST: TRK, TKGMN=a-b&&b

TST: TRK, TG=a

NOTE: For parameter options see 235-600-700, *Input Messages Manual*.

7.2 MANUAL TRUNK CONVERSION PROCEDURES

7.2.1 Planning Manual Trunk Conversion

Any ISUP trunk groups must be identified to the service provision systems and circuit identification codes assigned to each member of the trunk group. Table 7-1 contains the example planning data needed to manually convert PTS trunks to the SS7 trunks. The values shown in Table 7-1 must be the same at both ends of the trunks.

Table 7-1 Example Manual Trunk Conversion Planning Data

PER TRUNK SIGNALING GROUP	MEMBER	CLCI TM CODE TRUNK ID ^a	SS7 GROUP	MEMBER	CIRCUIT ID CODE TRUNK ID ^a
300	0	2000	425	0	4020
300	1	2001	425	1	4021
300	2	2002	425	2	4022
Notes:					
a. The values indicated in this table must be common for both ends of the trunks.					

In the switch, the CLCITM code trunk identification field is used for ISUP trunk circuit identification code value. For trunks connecting to a far-end office (destination code), the circuit identification code values must be a unique 4 digits among the trunk set.

NOTE: The trunk circuit identification code value can be from 0 to 9999. For the latest information, refer to 235-080-100, *Translation Guide*.

It is recommended that rather than use the existing CLCITM code trunk identification that a defined planning approach be used to assign circuit identification code trunk identification codes.

7.2.2 Implementing Manual Trunk Conversion

The PTS trunk manual conversion process involves deleting each trunk from the switch trunk group and reinserting it in a new SS7 trunk group. After all PTS trunk group members have been deleted, the PTS trunk group and the group data is deleted from the switch routing data.

To avoid loss of traffic, manual conversion should be during a low traffic period. The conversion strategy will depend on the size and routing of the trunk group. The following are some suggested approaches:

- The route index pointing to a trunk group and then to another route index and trunk group indicates that the second trunk group is an overflow group. The overflow group may be converted and then, by taking members from the first group out of service, a load may be introduced to the new CCS group.
- If the route overflow index does not exist, one may be created and pointed at the new CCS group to be built from members of the first PTS group on this route.
- It may be desirable to delete 50 percent from a PTS group, add them to the new CCS group, and direct the route index pointer to the new group. This will allow calls to be routed back to the old group during the remainder of the conversion.
- The last approach is to delete all members of a PTS group, change the group data to make the group ISUP, then reinsert the members as SS7 members.

Regardless of the approach used, the trunk group members should be reused, where possible, and route index entries for the conversion kept to a minimum. Some of the concerns to consider are as follows:

- All routes involving conversion groups must be known.
- Trunk group numbers 1 through 999 must be converted before higher numbered groups.
- To help verify routing, the relation `RT_ROUTING` may be batch reviewed.

7.2.3 Removing Trunks From Service

When a block of PTS trunks have been identified for conversion, the trunks may be removed from service with the following messages:

- `RMV:TRK, TKGMN=a-b&b` - This message removes a trunk or a range of trunks.
- `RMV:TRK, TG=a` - This message removes the group.
- The remove message is used with the out of service (OOS) and circuit administration (CADN) as parameters. To verify that all group members are OOS and meet the CADN requirement, an output list message (`OP:LIST, TG=a, FULL, PRINT;`) may be used.

7.2.4 Recent Change Data

7.2.4.1 Recent Change View 10.2

Recent Change (RC) View 10.2 may be used to change the trunk group to which a route index is pointing, or to provide a secondary route index.

7.2.4.2 Trunk Group Data

When creating a new CCS group, the RC View 5.1 is used. The view may be updated if the new CCS trunk group is being created from an old PTS group. Only the fields needed to change the group from a PTS group to a CCS group will be presented; the fields not presented are either self-explanatory or do not apply to CCS.

The **trunk direction (TRK DIR)** may be incoming, outgoing, or two-way, even though they are equipped for one-way signaling. One-way signaling is accomplished by inserting routing data at only one end of the trunk. The CCS field patterns in the trunk data are as follows:

	FAR CLLI = (Far-end CLLI code) TRK DIR = Incoming, Outgoing or Two-Way HUNT TYPE = 1WF, 1WB, 2WF, 2WB, LGBD, OR LGFD GLARE YLD = N INC TNDWNK = N INPLS AND OUTPLS = ISUP NCD SCRIN = NONE ORIG LATA = 0
Fields under CCS TRUNK heading:	TRK QUERY = Y TRANS TEST = Y VPA RATE = 100 (This rate may be decreased later) VPA TYPE = (Depends on type of facility) NEAR CLLI = (Near-end CLLI code)
Fields under CCITT7 heading:	DEST PT CODE = (Far-end point code for the group) ORIG PT CODE = (Near-end point code for the group)

Any values or optional values may be found in 235-118-213, *Recent Change Menu Mode Document*.

7.2.4.3 Trunk Member Data

After the group data has been inserted or updated, the members of the CCS group may be updated and inserted into the group by using the RC View 5.5 or 5.10 and equivalent recent change test, as required. The following are the trunk member field patterns:

CLCI TRK ID =	(Planned circuit identification code)
IDLE STATE =	ON
INSTART DIAL =	NONE
OUT START DIAL =	NONE
CCIS6 TRUNK =	N

If new fields appear that are not understood or if input values are in question, see 235-118-213, *Recent Change Menu Mode Document*.

7.2.5 Transceiver - Equipage Information

7.2.5.1 Pregrowth

This information applies to offices with digital service unit (DSU2), LDSU1-2 (upgraded LDSU1 with TN1637 packs), or module controller (MCTU2) type of units. The new MCTU2 has the digital service circuit on the shelf with the controller. The TN833 packs equipped in either of these units (DSU2 or MCTU2) must be microcode MC5D085A1 or later. This is the pumpable TN833. The TN1637 packs equipped in the LDSU1-2 should be microcode MC5D14091.

The amount of transceivers to equip is based upon the number of SS7 trunks in the switch module. The recommended amount of transceivers is five per service group, or ten per switching module with SS7 trunks. The average holding time of a transceiver is 350 ms. If a switch module is to be fully equipped with SS7 trunks, more than ten transceivers may have to be assigned.

7.2.5.2 TN833 or TN1637 Assignment

The RC View 20.21 is used to assign different functions to the digital signal processors on the circuit pack. RC View 20.21 has the following fields:

- Switching Module (SM)
- Digital Service Unit (DSU), enter 0
- Service Group (SG)
- TYPE (assignable function type)
- SERVICE CNT (count of available function type).

There are two maximums that limit the assignments of the functions. The maximums that may not be exceeded are time slots per service group and function type per digital signal processor. The assignments of the functions are as follows:

- There are 32 time slots per service group; each time slot has a receive and a transmit side.
- There are two receiver slots and one transmit slot used for control and maintenance.
- The remaining slots are the assignable maximums (30 receive slots, and 31 transmit slots).

The four functions that may be assigned are as follows:

- (1) Tone Generation (LDSU2TG) - uses one transmit slot per service count.
- (2) Tone Decoding (LDSU2TD) - uses one receive slot per service count.
- (3) Tone Transceiver (LDSU2TX) - uses one receive and one transmit slot for each service count in Field 5 of RC View 20.21.
- (4) CAMA Transfer Decoder (LDSU2CTD) - uses one receive slot per service count.

Neither the sum of the receive nor the sum of the transmit slots may exceed the service group maximums. A fully assigned digital service circuit is identified per the following chart:

COUNT	FUNCTION
31	LDSU2TG
30	LDSU2TD

A digital service circuit with transceivers is identified per the following chart:

COUNT	FUNCTION
26	LDSU2TG
25	LDSU2TD
5	LDSU2TX

Both examples show maximum assignment of the available service group slots. If the TN833 circuit is fully assigned, the counts of the other functions must be reduced.

In order to move from the first example to the second, it would require the following:

- Remove the LDSU 0, service group 0, from service.
- On View 20.21, change Field 5 from 31 to 26, for type LDSU2TG and update.
- On View 20.21, change Field 5 from 30 to 25, for type LDSU2TD and update.
- On View 20.21, insert type LDSU2TX and a count of 5.
- Restore the LDSU.
- After service group 0 is restored, the same steps may be executed on service group 1.

There are two other views that must be checked to assure that voice path assurance and continuity tests will run. They are Views 14.1 - Trunk Test Table, and 5.1 - Trunk Group. For View 14.1, a table must be assigned to the SS7 trunk group and the table must have Field 18 - Test Code set to CONT. For View 5.1, the following must be checked:

FIELD	NAME	VALUE
63	TRK QUERY	Y
64	TRANS TEST	Y
65	VPA RATE	Percent if set to 100, the trunks in this group will be tested every time they are seized.
66	VPA TYPE	This is two- or four-wire and describes the far-end office.

7.2.6 Performing Recent Changes

7.2.6.1 Begin Recent Change

Recent change work can begin after taking the trunks to be converted out of service. The review portion may be performed prior to taking the trunks out of service.

The data operations may be performed via recent change screens, recent change view (RCV) terminals, or from the operating support system via recent change text. View numbers and an example of text input are given in this section.

Some of the data capabilities of the switch should be used during this conversion phase. The RC View 5.1 may be used to update necessary group data on all members of a group. The View 5.5 is the trunk member view which has a quantity (QTY) field that may be used to perform an operation on a range of trunks. The trunk member view may be used to delete a step of the conversion. The View 5.10 is the trunk copy view which should be used for inserting the new CCS trunk members.

The following is a guide for performing recent changes:

- Review the trunk member data and hold values in memory for an automatic operations support system. The quantity field in the RC View 5.5 may be used.
- Delete designated PTS trunks that are already out of service. The RC View 5.5 quantity field may be used.
- Create the new CCS group, or update the PTS group with CCS data. The PTS group to be updated would be a group with all members deleted. The RC View 5.1 is used for this change.
- Insert new CCS members using data from review of old members after the update of proper value pairs. The Recent Change View 5.10 (trunk copy) may be used.

Repeat the previous steps for each trunk in the conversion block. Similar action must be occurring at the far-end switch, and must be completed before proceeding to the translation test step.

7.2.6.2 Translation Test

All of the remaining actions required in the trunk conversion process must be coordinated with the far-end switch.

Perform a demand translation test for each trunk in the conversion block. To initiate the CCS translation test interoffice audit for CCS trunks, use the following command:

```
AUD;CCSXLATE,TKGMN=a-b;
```

The audit will ensure that the far-end switch knows about the circuit identification code value that has been assigned to each trunk. Interchanged circuit identification codes may only be detected by a continuity test performed next.

7.2.6.3 Trunk Test and Turnup

The trunks inserted using recent changes are in the out-of-service, circuit administration (OOS,CADN) state. Tests and query commands may be run on the trunks while they are in this state. The demand trunk query is run first to mark each trunk state *blocked at both ends*. While in the blocked state, the response to the other end is *locally blocked and remotely blocked*. The command to accomplish this is as follows:

```
AUD:CCSTQ,TKGMN=a-b;
```

The telephone company's policies designate the office that is to control the turnup of each trunk group. The controlling office will run a test call using the following command:

```
TST:TRK,TKGMN=a-b;
```

This will have an effect of executing an operational test call on the trunk. If the trunk fails the operational test call,

the problem is likely to be in the data of either the near-end or far-end office. After a successful audit and test call, the controlling office may restore the trunks using the following commands:

```
RST:TRK,TKGMN=a-b,OOS,CADN,UCL
```

If necessary, data may be moved to route calls over the new CCS group.

7.2.7 Recent Change Text Example (Job Aid)

The following is only an example. The actual input for conversion will require many more value pairs.

3RCV:APPTEXT! Next, turn off screen format.

VFYNMVAL! This is to be executed from an automatic system which is external to the switch and has access to the recent change text interface channel.

Review and save data for the per-trunk signaling (PTS) trunks to be converted. This trunk member data should be saved in the memory of the operation service system for later use. The major part of the data will be reinserted after minimal changes to reflect CCS type trunk members.

Step 1 Verify.

```
FORM=5v5,VFY!
```

```
TKGN=300!
```

```
MEMBNBR=0!
```

```
QTY=01!
```

```
VFY!
```

Step 2 Delete the trunk from its PTS group.

```
FORM=5v5,OUT!
```

```
TKGN=300!
```

```
MEMBNBR=0!
```

```
QTY=01!
```

```
OUT!
```

Step 3 Create the new trunk group, or update the old PTS group data to convert the group to CCS.

```
FORM=5v1,NEW!
```

```
TGN=425!
```

```
INPLS=ISUP!
```

```
OUTPLS=ISUP!
```

```
NEW!
```

Step 4 Insert the trunk members in the SS7 group. Values used were from the verification done in Step 1

with changes made to specific fields to make the trunk SS7.

FORM=5v5, NEW!

TKGN=425!

MEMBNBR=0!SET="EN.TENTYP"&D"EN.entrk1"&001003001

CLCITRKID=4020!

IDLESTATE=ON!

INSTARDIAL=NONE!

NEW!

END!

NOTE 1: Many name value pairs are required, but not shown. Most of the data comes from the verify Step 1.

NOTE 2: Steps 1, 2, and 4 should be done for each trunk; Step 3 need only be done once to create the CCS trunk group. Steps may be modified to take advantage of the QTY field and trunk member copy.

NOTE 3: The data and messages here are for example only; users must reference 235-118-212, *Recent Change Procedures Text Interface*.

7.3 AUTOMATED TRUNK CONVERSION

7.3.1 Description

The Simultaneous Trunk Conversion via Automatic Recent Change (STAR) library program provides network service personnel with a process for the conversion of trunks from Per-Trunk Signaling (PTS) protocol to Signaling System 7 (SS7) protocol. The STAR process places test calls from a HOST office to a REMOTE office to determine the connectivity between the offices. When the remote office detects the test call, it responds with the connectivity data back to the host office. The host office then makes up the appropriate recent change (RC) messages that cause the trunk to be converted from PTS to SS7 protocol in each office. The STAR process continues to access trunks until each designated trunk or trunk group is converted.

The Enhancements for STAR feature provide the remote STAR library program with the ability to detect an incoming STAR test call outpulsed from the host switch.

The Enhancements for STAR feature along with the STAR library program increase the speed of conversion processing (the conversion can convert up to four trunk members per minute without interfering with ongoing services). This feature also extends the automatic SS7 trunk conversion process to any combination of 5ESS[®]-2000 switch and 1A ESSTM switch.

7.3.2 Availability

The STAR library program is available with 5E6 and later software releases.

NOTE: Consult your Lucent Technologies Account Executive for availability.

7.3.3 Feature Provision Basis

The STAR library program and Enhancements for STAR feature are provided on a per-office basis.

7.3.4 User Perspective

7.3.4.1 User Profile

The Enhancement for STAR feature is transparent to the end user. Maintenance personnel use this feature and the STAR library program to automatically convert PTS trunks to SS7 protocol.

7.3.4.2 User Operation

Telephone company personnel load STAR library programs into the host and remote switches. When the STAR programs have been loaded, the following options are available for selection:

- Initiate a switch-STAR conversion session on a trunk-by-trunk basis.
- Initiate a switch Check Only STAR (COSTAR) session on a trunk-by-trunk basis.
- Initiate a switch-STAR conversion session on a trunk group at a time basis.
- Initiate a switch Check Only STAR (COSTAR) session on a trunk group at a time basis.
- Pause a trunk group at a time type of switch-STAR session.
- Restart either type of just paused switch-STAR session.
- Provide optional magnetic tape output from either type conversion session.

For detailed office preconditioning and operating procedures when using the STAR library program, refer to 256-015-310, *Simultaneous Trunk Conversion via Automatic Recent Change for 1A ESSTM Switches or 5ESS[®]-2000 Switches*.

7.3.4.3 Operational Limitations

The programmed assignment of circuit identification codes (CICs) is not supported in the switch STAR library program.

7.3.4.4 Interactions

The enhanced STAR automatic trunk conversion does not interfere with ongoing services.

7.3.5 Engineering - Hardware

Each office involved in the STAR session must have an operational Common Network Interface (CNI) with links to a Signal Transfer Point (STP). Signaling between the host and remote offices is via an input/output (I/O) device. It is recommended that the I/O device at each office be assigned to a 1200-baud full duplex channel. The I/O device can be established by acquiring a voice line and attaching 212A data set compatible modems to each end and informing the switches software release programs of the presence of the device and its use. A simplified STAR hardware configuration is shown in Figure 7-1.

NOTE: For detailed connection procedures when using the STAR library program, refer to 256-015-310, *Simultaneous Trunk Conversion via Automatic Recent Change for 1A ESSTM Switches or 5ESS[®]-2000 Switches*.

7.3.6 Assignment Guidelines - Forms and Views

7.3.6.1 Translation Guide Forms

If the `WETESTC` value is used in the destination type during a retrofit or large terminal growth, the ODA process does not recognize it as a valid value and deletes it.

7.3.6.2 Recent Change Views

No RC view masks are changed because of the Enhancements for STAR feature. The following views have the value `WETESTC` added as a valid value to the CALL TYPE field:

- RC View 9.3, Local Digit (Office Dialing)
- RC View 9.15, Multiple Local Digit (Office Dialing).

On RC View 9.3 (or 9.15), define the local digit interpreter table and specify `WETESTC` in the CALL TYPE field for the incoming digits associated with the STAR test call.

7.3.7 System Operation

The enhanced STAR feature detects incoming STAR digits at the remote office and sends trunk and office information to the STAR library program via the Library Request Administrator (LRA). The following steps and Figure 7-2 summarize the call processing events when using this feature:

- (1) The incoming STAR test call enters the switch remote on the PTS trunk group member(s) to be converted to SS7 signaling.
- (2) The call is passed to standard switch incoming trunk call processing.
- (3) Digit analysis determines the incoming digit string that is associated with the call type `WETESTCAL`.
- (4) A route request message is sent to the LRA system.
- (5) After the message is sent to the LRA, the call is sent to reorder.

7.3.8 Administration

Not applicable.

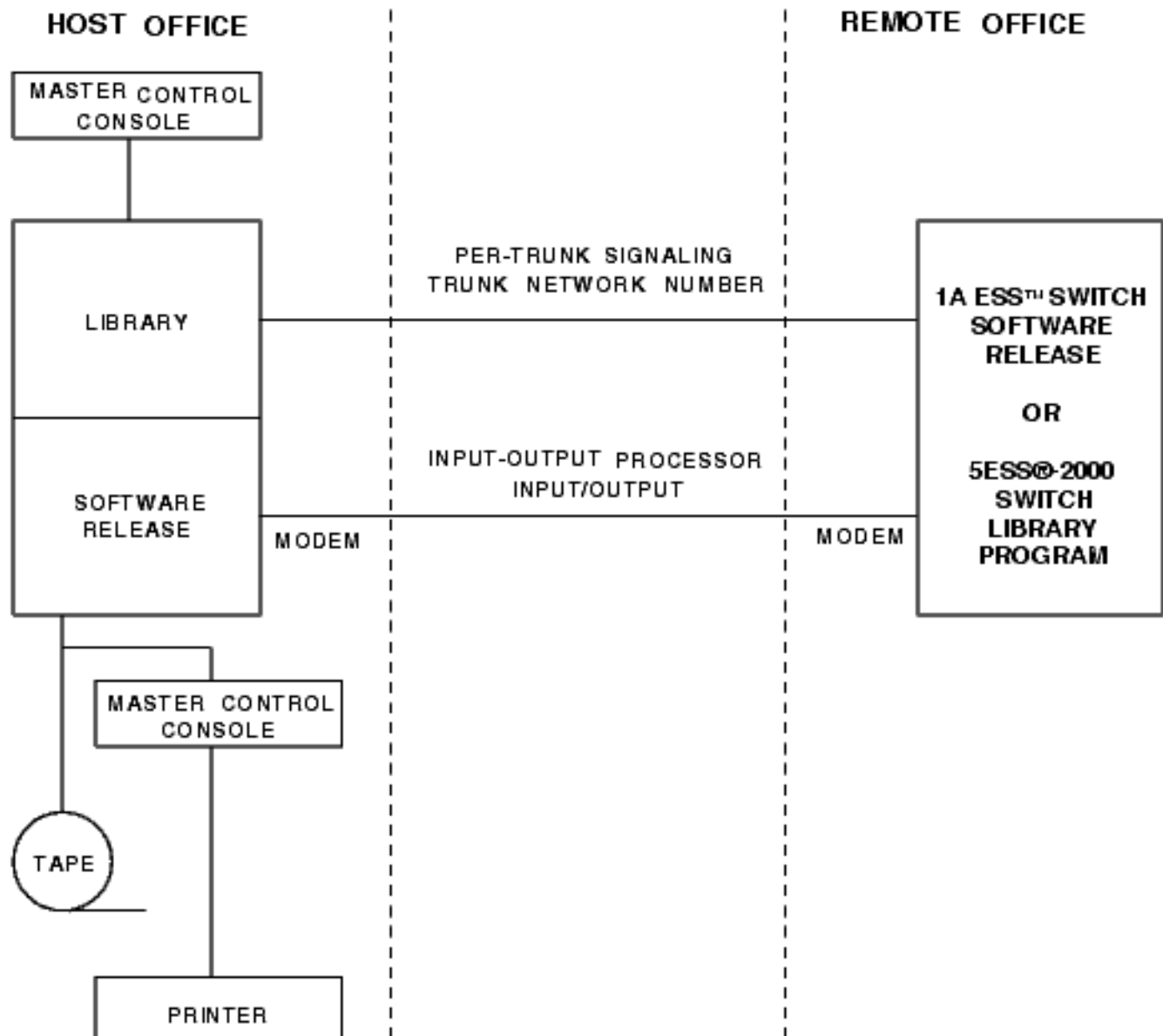


Figure 7-1 STAR Hardware Configuration

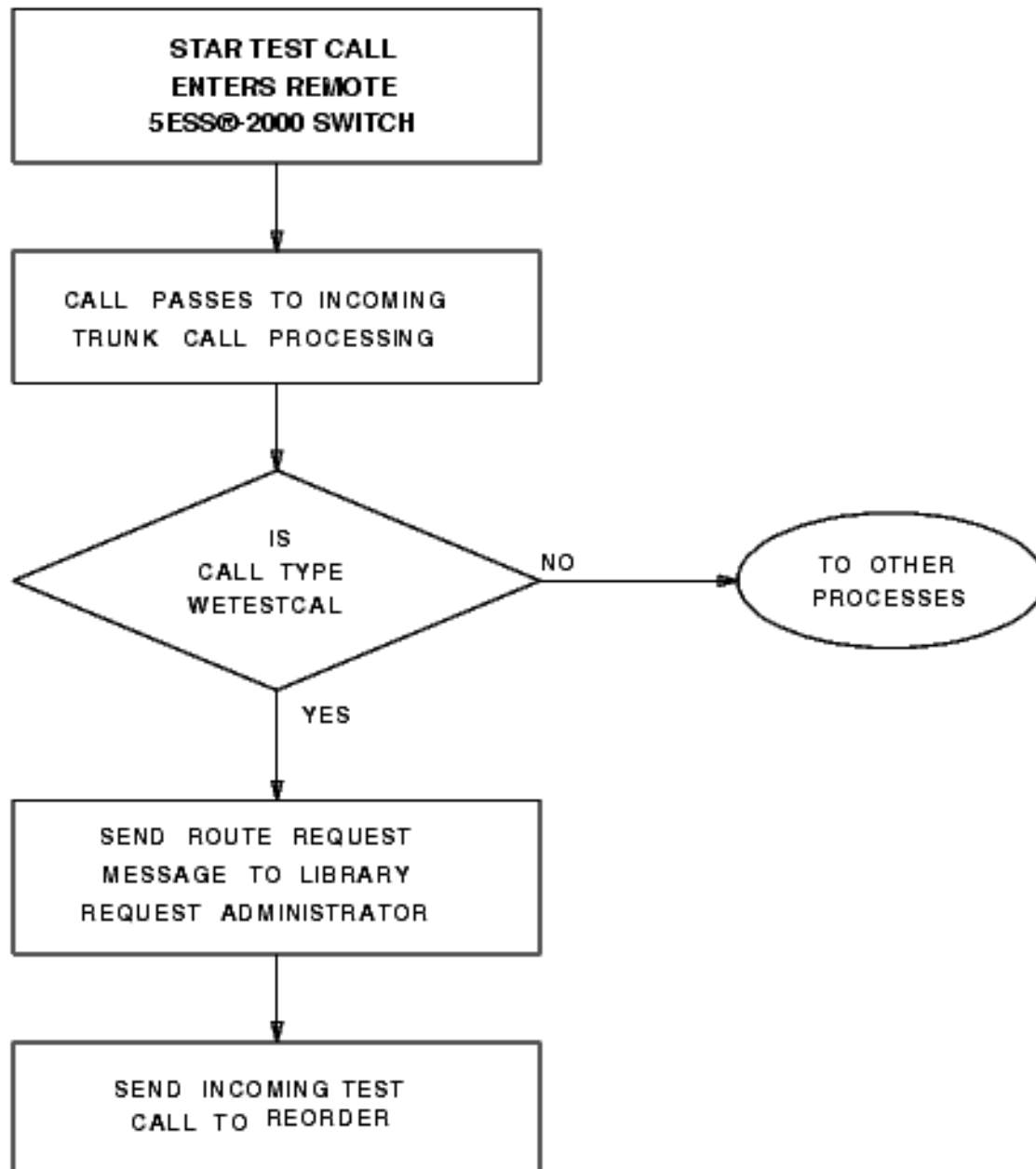


Figure 7-2 Enhanced STAR Call Data Flow Diagram

8. PROBLEM IDENTIFICATION

The purpose of this section is to aid switch personnel in the 5ESS[®]-2000 switch office with running diagnostics on the common network interface (CNI) ring and various Common Channel Signaling (CCS) features.

8.1 MESSAGE TRAP FEATURE

8.1.1 Description

The Message Trap feature provides the capability of collecting and printing SS7 messages coming in from the signaling network via the common network interface (CNI) ring nodes. It is intended to aid in the detection of signaling protocol problems but is not a full protocol analyzer with extensive processing capability. It is intended to be used in selected situations where specific data can be trapped within the processing capabilities provided. For more detail on how to use the tool, refer to 256-015-300, *Signaling System 7 LEC Network Operations, Administration, and Maintenance*.

8.1.2 Availability

The Message Trap feature was available with the 5E6 software release. This initial deployment of Message Trap only supported the "incoming" mode. In the 5E7 software release, the enhanced version of Message Trap was deployed. This version of Message Trap also supported the "outgoing" mode.

8.1.3 Message Trap Characteristics

8.1.3.1 Capabilities and Limitations

The capabilities and limitations of the Message Trap feature are as follows:

- Incoming messages are trapped on SS7 nodes. Incoming messages on SS7 nodes that are routed to signaling routing node (SRN), and are discarded or returned to the CCS network, are trapped at the SRN. If some users of CNI do not have SRN in their configuration of the CNI ring, trapping is not available for returned or discarded messages.
- Up to five simultaneous active Message Traps are given at any time.
- No more than 32 traps may be entered during a 24-hour period. If an attempt to enter more than 32 traps is made, switch personnel need to remove some of the earlier message trap commands.
- Each message trap activates on any of the links, but all active message traps may affect a maximum of 40 links at any given time. Switch personnel can specify a range of links, list of links, or a linkset in each message trap command.
- There can be only one active trap per link.
- For trapping the desired messages, up to 5 fields within a message are specified [for example, originating point code (OPC) and destination point code (DPC)]. If more than one condition is specified, all conditions must be satisfied for the message to be trapped. Switch personnel may also specify an offset and a bit-pattern to be matched as one or more of the five fields for trapping a message.
- Message fields of higher layers of protocols [such as, Integrated Services Digital Network User Part (ISUP), Transaction Capability Application Part (TCAP), Data User Part] may be given in the input commands.
- Switch personnel can specify the rate of matching messages (1 out of N) to be collected. For example, if N is specified as 50, 1 out of every 50 matching messages is collected.
- A Message Trap is started immediately or at any half-hour boundary during the next 24 hours. Craft gives duration or a count of desired number of trapped messages, after which the trap is terminated. An active or pending trap terminates explicitly by a `STOP:TRAP` command.
- Once started, a Message Trap is active for 24 hours.

- Trapped messages are printed out in real time during the trap. They print at the termination of the trap by the `OP:TRAP` command. In addition, all the results of a trap command are stored in a disk file, and the results are preserved for at least 24 hours after the termination of the trap.
- The results are printed out in hexadecimal dump, along with some of the relevant fields (for example, OPC and DPC) being printed out in user-friendly format.
- The trap(s) is terminated at any time when resources (memory or real time either at the nodes or at the AM) are exhausted. A diagnostic message is printed explaining the reason for termination of the trap.

8.1.3.2 Initialization

All active Message Traps are terminated during CNI level 3 or 4 initialization of the AM. Message Trap results that are stored in incore buffers at the AM is lost (that is, a loss of a maximum of 3 minutes of trapped messages). Results that were backed up in the disk file remains available. No diagnostic message for termination of the traps is printed because the MCC is also down during CNI initialization.

8.1.3.3 Aborting a Message Trap

A Message Trap automatically aborts for several reasons, but usually, it aborts because of resource exhaustion. All traps abort at the AM for any one of the following reasons:

- `Mon_trap` is killed.
- CNIINIT sends a `_STOP_PROC` event to `mon_trap`.
- Nodes send too many trapped messages and the frequency of writing messages, from AM incore buffers to the disk file, gets higher than some thresholds.

An active trap in an SS7 node is aborted for any one of the following reasons:

- Both trap buffers in the node are full. This happens when the rate of trapping specified in the input command is too high.
- Overload congestion in the receive buffers in DPRAM. When the node processor is not picking up messages as fast as they are queued by the link interface, congestion results in DPRAM.
- First level of congestion in the ring receive buffers in the transmit direction. The messages received from the ring are stored by IMS in the ring receive buffers. The CNI processes these messages at interrupt-level, along with the messages arriving from the network. Normally, congestion of ring receive buffers should not occur due to message trap work, because the ring interrupt has priority over the link interrupt. An active trap aborts in the node if there is any congestion in the ring receive buffers because congestion would occur due to the lack of real time in the node processor (NP) or the link interface (LI).
- First level of congestion in a ring peripheral control (RPC) node. All trapped messages are sent from the nodes to the AM by using an RPC node. It is important to guard against flooding the AM with too many trapped messages.
- Trapped messages returned from the AM. If the AM returns a trapped message to the node, it is due to a lack of IMS buffer space in the AM, or some other reason (such as, channel not open). In any case, when a node receives a returned message, the trap aborts.

8.1.4 Software Architecture

In order to implement the Message Trap feature, software is written for the AM, SS7 node, and SRN.

Switch personnel enable/disable a trap from the master control center (MCC), or for remote operations, by using a specified operations system (for example, SCCS). These commands are processed at the AM. An AM *UNIX*® system level process performs preliminary checks on the validity of the input command and sends the trap command along with all the attributes to the nodes specified in the command.

When a trap in a node has been activated, all incoming messages in the node are matched against the trap attributes. Some or all of matching messages (as specified by the rate in the input command) are collected in a buffer. Periodically, the buffer is sent to the AM, where the messages are collected in another buffer. An AM *UNIX*® system level process writes, periodically, the trapped messages into a disk file. The trapped messages are printed out on the output device specified in the input command. The default output device is where the input command was entered. Switch personnel may specify the output device to be either MCC, receive-only printer (ROP), or a specified operation system (for example, SCCS). Results in the disk file are saved for 24 hours, unless they are purged by switch personnel.

8.1.5 Message Trap Input Commands And Processes

This section details how each node type and the AM is implemented. The message trap input commands and processes are as follows:

NOTE: For a detailed description of messages, format, and parameters, refer to 235-600-700, *Input Messages Manual*.

- SET:TRAP
- ALW:TRAP
- INH:TRAP
- STOP:TRAP
- OP:TRAP
- MON_TRAP.

8.1.5.1 SET:TRAP Command

The SET:TRAP command activates the AM process `set_trap` and allows the maintenance person to enter all the parameters of a trap command. The trap starts immediately if the `start_time` is not specified in this command. Parameters that specify bit patterns may be entered in decimal or hexadecimal, except the global title fields which can only be entered in hexadecimal. This command may also be entered in a file for ease of use.

NOTE: For entry format and parameters, refer to the SET:TRAP command in 235-600-700, *Input Messages Manual*.

The process `set_trap` checks first whether the start trap command is valid. It also checks whether the parameters are appropriate or not. A SET:TRAP command may contain some higher-level fields in symbolics that are parsed by the application. An interface needs to be worked out with the application. If there is any error in the input command, the command is rejected and a diagnostic message is printed on the output device. If the trap command is set on a node which is out of service, it is rejected with a diagnostic message. However, if the node is in service but the link is out of service, the start trap command is accepted because it may need to trap the messages received immediately after the link is brought into service.

If a valid command is received, `set_trap` process sends the acknowledgement print follow (PF) that the command was accepted. It then checks to see if the process `mon_trap` is in existence. The `mon_trap` process may be in the process of recreation by `CNIINIT`. If `mon_trap` is not running, `set_trap` prints out a diagnostic message telling the maintenance person to try the command later and then terminates itself.

If `mon_trap` is running, `set_trap` sends an RTR message to `mon_trap` which contains all the information for a given trap. It receives a trap identification from `mon_trap` and prints it out on the output device. This trap identification is used to identify the trap in any other command. If `set_trap` does not receive a trap identification from `mon_trap`, it prints out a diagnostic message telling the maintenance person to try the command later and then terminates itself. If `set_trap` receives the trap identification from `mon_trap`, it prints out the trap identification and then terminates itself.

A separate `set_trap` process is created for each `SET:TRAP` command. Multiple copies of the `set_trap` process may exist if multiple `SET:TRAP` commands are entered at the same time.

8.1.5.2 ALW:TRAP Command

This transient command creates the AM process `alw_trap`. It allows the maintenance person to start a trap that was entered by the `SET:TRAP` command or to resume a trap that was suspended by the `INH:TRAP` command. This process is created when the `ALW:TRAP` command is entered. It restarts a trap that was aborted or was stopped because the duration or message count criterion was fulfilled.

NOTE: For entry format and parameters, refer to the `ALW:TRAP` command in 235-600-700, *Input Messages Manual*.

There is only one parameter for the `ALW:TRAP` command. The parameter specifies one or more trap identification(s) for the trap(s) that should be started or resumed. A value of `ALL` starts all suspended/pending traps.

This process first checks the validity of the `ALW:TRAP` command. If the command is invalid, it is ignored and an error message is printed. An acknowledgement (OK) for a valid command is printed on the device where `ALW:TRAP` command was entered. It then checks to see if the process `mon_trap` is in existence. The `mon_trap` may be in the process of recreation by `CNIINIT`. If `mon_trap` is not running, `alw_trap` prints out a diagnostic message telling the maintenance person to try the command later and then terminates.

If `mon_trap` is running, `alw_trap` sends an RTR message to `mon_trap` that contains the input command. It waits to receive an acknowledgement RTR message from `mon_trap`. If `alw_trap` does not receive an acknowledgement from `mon_trap`, it prints out a diagnostic message telling the maintenance person to try the command later and then terminates. If `alw_trap` receives the acknowledgement from `mon_trap`, it terminates.

A separate `alw_trap` process is created for each `ALW:TRAP` command. Multiple copies of the `alw_trap` process may exist if multiple `ALW:TRAP` commands are entered at the same time.

8.1.5.3 INH:TRAP Command

This transient command creates the AM process `inh_trap`. It allows the maintenance person to temporarily suspend an active trap. It is created when the `INH:TRAP` command is entered.

NOTE: For entry format and parameters, refer to the `INH:TRAP` command in 235-600-700, *Input Messages Manual*.

There is only one parameter for the `INH:TRAP` command. This parameter specifies one or more trap identification(s) for the trap(s) that should be suspended. A value of `ALL` suspends all active traps.

This process first checks the validity of the `INH:TRAP` command. If the command is invalid, it is ignored and an error message is printed. An acknowledgement (OK) for a valid command is printed on the device where `INH:TRAP` command was entered. It then checks to see if the process `mon_trap` is in existence. The `mon_trap` may be in the process of recreation by `CNIINIT`. If `mon_trap` is not running, `inh_trap` prints out a diagnostic message to say that all the traps are aborted due to reinitialization.

If `mon_trap` is running, `inh_trap` sends an RTR message to `mon_trap` which contains the input command. It waits to receive an acknowledgement RTR message from `mon_trap`. If `inh_trap` does not receive an acknowledgement from `mon_trap`, it prints out a diagnostic message informing the maintenance person to try the command later and then terminates. If `inh_trap` receives the acknowledgement from `mon_trap`, it terminates.

A separate `inh_trap` process is created for each `INH:TRAP` command. Multiple copies of the `inh_trap` process may exist if multiple `INH:TRAP` commands are entered at the same time.

8.1.5.4 STOP:TRAP Command

This transient command creates the AM process `stop_trap`. It allows the maintenance person to stop an active or a pending trap. This process is created whenever the `STOP:TRAP` command is entered.

NOTE: For entry format and parameters, refer to the `STOP:TRAP` command in 235-600-700, *Input Messages Manual*.

This process first checks the validity of the `STOP:TRAP` command. If the command is invalid, it is ignored and an error message is printed. An acknowledgement (PF) for a valid command is printed on the device where `STOP:TRAP` command was entered. It then checks to see if the process `mon_trap` is in existence. The `mon_trap` may be in the process of recreation by `CNIINIT`. If `mon_trap` is not running, `stop_trap` prints out a diagnostic message informing the maintenance person that all traps are aborted due to reinitialization.

If `mon_trap` is running, `stop_trap` sends an RTR message to `mon_trap` that contains the input command. It waits to receive an acknowledgement RTR message from `mon_trap`. If `stop_trap` does not receive an acknowledgement from `mon_trap`, it prints a diagnostic message informing the maintenance person to try the command later and then terminates. If `stop_trap` receives the acknowledgement from `mon_trap`, it terminates.

A separate `stop_trap` process is created for each `STOP:TRAP` command. Multiple copies of the `stop_trap` process may exist if multiple `STOP:TRAP` commands are entered at the same time.

8.1.5.5 OP:TRAP Command

This transient command creates the AM process `op_trap`. It allows the maintenance person to output the results of an active-inhibited or a previously completed trap. It creates when the `OP:TRAP` command is entered. The `OP:TRAP` command allows the maintenance person to obtain information on traps that are active/pending or about the intermediate results of an active trap.

NOTE: For entry format and parameters, refer to the `OP:TRAP` command in 235-600-700, *Input Messages Manual*.

This process first checks the validity of the `OP:TRAP` command. If the command is invalid, it is ignored and an error message is printed out. An acknowledgement (PF) for a valid command is printed on the device where `OP:TRAP` command was entered. It then checks to see if the process `mon_trap` is in existence. The `mon_trap` may be in the process of recreation by `CNIINIT`. If `mon_trap` is not running, `op_trap` prints out a diagnostic message informing the maintenance person to try the command later, and then terminates.

If `mon_trap` is running, `op_trap` sends an RTR message to `mon_trap` that contains the input command. It waits to receive an acknowledgement RTR message from `mon_trap`. If `op_trap` does not receive an acknowledgement from `mon_trap`, it prints a diagnostic message informing the maintenance person to try the command later, and

then terminates. If `op_trap` receives the acknowledgement from `mon_trap`, it terminates. The `mon_trap` process is responsible for passing the results of the `OP:TRAP` command to the output device.

A separate `op_trap` process is created for each `OP:TRAP` command. Multiple copies of the `op_trap` process may exist if multiple `OP:TRAP` commands are entered at the same time.

8.1.5.6 MON_TRAP Process

This noncritical process is a child of the CNIINIT process. It is responsible for sending the trap commands to the nodes, storing the trapped messages in the AM processor memory, and maintaining information on the active, pending, and some of the previously completed traps.

There is only one copy of the `mon_trap` process; whereas, multiple copies of the five transient processes exist if more than one instance of a command is entered simultaneously.

8.1.5.7 RESOURCE MANAGEMENT

The message trap feature is an aid to assist in isolating problems in the CCS network. It does not hamper the normal processing of signaling messages at the nodes nor the normal functions at the AM. Real time and memory are monitored and the traps can be aborted if the resource usage is in danger of affecting normal call processing.

Real time, incore memory, disk memory, node real time, and node memory are at the AM.

All message trap processes in the AM run at *UNIX*[®] system level (that is, real time is of less concern than memory at the AM).

Disk space must be available under the `/log/cni/mtrp` directory. At least 4K memory must be available in order for the feature to operate. On initialization, if the space is not available, the feature does not work.

8.1.6 OP:C7NET Command

This input command allows the routing information of the network to be examined upon request. The output is a formatted display of the routing data in the cluster, member, and load share tables of the common network and for the signaling connection control part (SCCP) subsystem bit map. This is useful in testing and monitoring the common channel signaling traffic management code that updates these tables.

The following are optional parameters for the `OP:C7NET` command:

- `PRTE` - Prints the contents of the routing data. This includes all pointcodes that do not have `NO_RTE` as a routing flag.
- `PREG` - Prints region data for all clusters in a given region, including cluster level data and any abnormal members. This command is always applied to a local network.
- `PCLU` - Prints data about a given cluster. For a remote populated cluster, only abnormal or congested members are printed. (An abnormal member has `pre/alt2/alt1 != TFA`.) For a local populated cluster, every member whose route flag `!= NO_RTE` is printed.
- `PMEM` - Prints out the member data for a given member.
- `PLS` - Prints link set information for a given equipped link set. The RNAs that are associated for that linkset and the current linkset are also printed.
- `STATES` - Gives the status of subsystems for a given point code.

- `DEBUGON` - Turns on the SCCP debug flag and request the SLMK process to print SCCP debugging information. As the SCCP processes subsequent stimuli, various types of debugging statements are printed.
- `DEBUGOFF` - Turns off the SCCP debug flag.
- `RIND` - Prints out the point codes of the two adjacent STPs, and indicates which local subsystems are marked as receiving backup traffic from each of these adjacent STPs.
- `BRDCST` - This will print all point codes which are contained in the SCCP broadcast list.
- `GTXTAB` - Prints the contents of the `cH7gtx_tab` table, which is used when selecting a global title translator point code.
- `SSINFO` - Prints out data about a given local subsystem.
- `LOCPC` - Prints the local point code.
- `RELATE` - Prints all point codes which are contained in the SCCP permanent relations list.
- `PFL` - Prints the free list for the particular table space and the length of elements to be displayed.
- `PFRNG` - Prints a range of integers, each representing marked free elements for the particular table.
- `PIDX` - Prints the indexing information in the nonlocal paging tables for a particular nonlocal point code.
- `PIDXMEM` - Prints the member level routing data indicated by index.
- `PRN` - Prints the cluster and member routing data for a particular network identifier.
- `PNID` - This option prints the network identifier data. For all networks that are assigned, the network level information is printed.
- `ABNORMAL` - This option will print the status of Common Channel Signaling System 7 (CCS7) signaling routes that have members that are unavailable, restricted, congested, or subsystems that are prohibited.
- `PIDXPA` - Print the entry in the `cNpage_access` table indicated by index.
- `PIDXNM` - Print the nonlocal routing data indicated by index.

8.2 CALL/CIRCUIT MONITOR FEATURE

8.2.1 Description

The Call/Circuit Monitor feature (99-5E-3114.B), hereafter known as the CCS Protocol Monitor (PM) feature, provides an on-demand request to monitor Common Channel Signaling (CCS) System 7 protocol messages for both the CNI and PSU platforms. The protocols supported are ISUP and TCAP. The raw hexadecimal output is provided as well as a text translation of the messages captured. Protocol monitoring is intended to aid in the detection of signaling protocol problems.

This feature's use is RESTRICTED until the purchaser has made the necessary financial arrangements with Lucent Technologies. Information on feature enabling will be provided upon ordering. Please contact your Lucent Technologies Network Systems Account Representative for ordering and pricing information. This is an OA&M secured Special Feature, and is controlled by secured feature number 260.

8.2.2 Availability

The CCS Protocol Monitor feature is available on the 5ESS[®]-2000 switch as a software update for 5E12, and is included in 5E13 and later software releases.

8.2.3 Environment

This feature is provided on a per-office basis.

8.2.4 Cross References

The following cross references apply to this feature:

- Feature Number: 99-5E-3114.B

8.2.5 Background

Not applicable.

8.2.6 Feature Operation

TCAP CNI-routed messages are captured in the Direct Link Node (DLN) of the CNI ring (if a DLN exists in the office). If no DLN exists, TCAP CNI-routed messages are captured in the AM. TCAP PSU-routed messages are captured in the SM. All ISUP messages (CNI- and PSU-routed) are captured in the SM.

The output from the PM session can be reported in hexadecimal format on the ROP or can be translated and stored in a text file on the AM. The file that contains the translated text output includes the raw hexadecimal format.

8.2.6.1 ISUP Capabilities

CCS PM provides the capability to monitor inbound and outbound ISUP messages. A CCS PM command is issued for a particular called or calling number. When an IAM with a specific called/calling number (inbound or outbound) is detected, PM starts recording messages. Subsequent messages for the call are matched based on the origination point code - destination point code - circuit identification code (OPC-DPC-CIC) values from the IAM. The session ends when one of the ISUP termination messages for CCS PM is encountered. The termination messages are Release Complete (RLC), Group Reset Acknowledge (GRA), and Unequipped Circuit Identification Code (UCIC).

CCS PM also detects glare situations for ISUP calls. If inbound and outbound IAMs with matching OPC-DPC-CIC values are recorded, a glare condition has occurred.

8.2.6.2 TCAP Capabilities

CCS PM provides a capability that records all messages related to a TCAP query transaction or global title routed unidirectional TCAP message for the following applications: Number Service 800 (NS800), Calling Name Delivery (CNAM), Advanced Services Platform (ASP), Advanced Intelligent Network (AINR0D1), Interswitch Voice Messaging (ISVM), and Local Area Signaling Services (LASS).

TCAP monitoring is performed on a transaction basis (in other words, a monitor session starts with the first message of a TCAP transaction and continues until the transaction has ended). In general, a TCAP transaction begins with a Query (QRY) message, is continued with any number of Conversation messages, and ends with a Response (RESP) message. The exception to this is the Unidirectional (UNI) message, which is the first and only message of the transaction.

For transactions that are initiated by the switch (transmit direction), messages can be monitored by matching on information in either the SCCP layer of the message or a combination of the SCCP and TCAP layers of the message. For transactions that are received by the switch (receive direction), messages can only be monitored by matching on information in the SCCP layer of the message. Note that matching is performed on the first message of the transaction, and if it is successful, all messages associated with the transaction are monitored.

Matching criteria and message layer are specified as options in the `exc:pmccs,tcap` command line.

The CCS PM command requires that either called or calling digits are specified with a choice of Called Party Translation Type, Called Party Subsystem Number, or Calling Party Subsystem Number. The direction of the message can also be specified (transmit, receive, or both — defaults to both) with the layer of the message used to match the digit information (SCCP or TCAP — defaults to SCCP). All of the criteria specified in the CCS PM command must match the message content in order to monitor the transaction.

8.2.6.3 Aborted CCS Protocol Monitor Session

A CCS PM session or recorder automatically aborts for several reasons, the most common being

- communication failure between processors,
- overload condition on a processor involved in the PM session, and
- DLN switch.

8.2.7 User Operation

8.2.7.1 For Subscribers

No subscriber actions are associated with this feature.

8.2.7.2 For Switch Personnel

The CCS PM feature aids in isolating problems in the CCS network. It does not hamper the normal processing of signaling messages at the links nor the normal functions in the AM. Real-time usage is checked, and the PM session is automatically stopped if its real-time usage is in danger of affecting normal call processing.

8.2.7.2.1 CCS Protocol Monitor Commands

For a detailed description of a CCS PM command, its format, and its parameters, refer to the 235-600-700, *Input Messages Manual*.

- **EXC:PMCCS** — requests that a CCS protocol monitoring session be started for the ISUP or TCAP protocol (based on the values of particular parameters in the command).
- **STP:PMCCS** — requests that a specific CCS protocol monitoring session or all CCS PM sessions be stopped.
- **OP:PMCCS** — requests a list of active CCS protocol monitoring sessions and provides status of the PM processors.

8.2.7.2.2 ISUP CCS PM Command Examples

- (1) Monitor on called number, direction = transmitted:

```
exc:pmccs,isup,called=6305551234,dir=xmt
```

Monitoring starts when an outbound IAM with called number 6305551234 is detected.

- (2) Monitor on calling number, direction = received:

```
exc:pmccs,isup,calling=6305556789,dir=rcv
```

Monitoring starts when an inbound IAM with calling number 6305556789 is detected.

- (3) `exc:pmccs,isup,calling=6305556789,dir=rcv,dur=30`

Same as Example 2, except that the monitoring session times out if not completed within 30 seconds.

- (4) `exc:pmccs,isup,called=6305551234,dir=xmt,repeat=1`

Same as Example 1, except that a second monitoring session starts after the first session completes.

8.2.7.2.3 TCAP CCS PM Command Examples

- (1) `exc:pmccs,tcap,called=630713,cgsn=250,layer=sccp`

Query or Unidirectional messages that contain both a Called Party Number (as Global Title Translation digits in the Called Party Address) of 630713XXXX and a Calling Party Subsystem Number of 250 are matched and begin a monitoring session. Messages that contain a point code in the Called Party Address (rather than global title digits) and a Calling Party Subsystem Number of 250 are not matched.

- (2) `exc:pmccs,tcap,called=8004501000,cdtt=53,layer=tcap`

Query or Unidirectional messages that contain both a Called Party Number (as Global Title Translation digits in the Called Party Address) of 8004501000 and a Calling Party Translation Type of 53 are matched and begin a monitoring session.

8.2.8 Engineering

8.2.8.1 Hardware Resources

No hardware considerations are associated with this feature.

8.2.8.2 Software Resources

No software considerations are associated with this feature.

8.2.8.3 Transition Considerations

No transition considerations are associated with this feature.

8.2.9 Interactions and Limitations

8.2.9.1 General Limitations

- (1) Only one PM session can be started simultaneously for each protocol.
- (2) There is a 2 Kbyte limit on the amount of data that can be recorded for a single PM session. When the 2 Kbyte limit is reached, the session terminates and the data is reported.

8.2.9.2 ISUP Limitations

- (1) CCS PM captures and records ISUP messages in the SMs before the messages are sent to the CNI/PSU platform. In case of outbound messages, the signaling link selection (SLS) value is changed in the CNI/PSU before the message is sent out to the network. CCS PM does not have access to this modified value. Hence the SLS is marked as "Unavailable" in the translated output for ISUP messages outgoing via the CNI/PSU platform.
- (2) The Calling Number Parameter in an IAM is an optional parameter. ISUP monitoring on a calling number does not record any messages if the calling number for a call is not present in the IAM.
- (3) CCS PM support on single-SM loop-around trunks (also called intra-module trunks or intra-IMTs) depends on the software release:
 - 5e12(1) — CCS PM is not supported for single-SM loop-around trunks. CCS PM may capture only messages received and not messages transmitted for ISUP calls over a single-SM loop-around trunk.
 - 5e13(1) and later — CCS PM is supported for single-SM loop-around trunks in a software update for 5e13(1) and in 5e14(1) and later software releases.

NOTE: For ISUP calls on a single-SM loop-around trunk, CCS PM captures *both* the transmitted and received instance of each message. For example, the CCS PM output will contain two copies of the IAM, two copies of the ACM, etc. The only difference between the copies will be their direction: one instance of the message will be XMT (transmitted) and the other instance of the message will be RCV (received). The session termination message (RLC, GRA, or UCIC) will be captured only once.

- (4) For ISUP calls, the called number input in the `EXC:PMCCS` command is matched with the Called Number Parameter in the IAM.

NOTE: An exception to the above statement occurs if an IAM is received with the Generic Address Parameter (GAP), and the Local Number Portability (LNP) feature is turned on in the switch where the IAM is received. In this case, the called number is matched with the GAP digits in the IAM. The GAP contains the actual dialed digits for the call.

- (5) For SS7 Multifarious Intra-Network Trunk (MINT) Gamma signaling, CCS PM traps on the called number digits, *not* on the Gamma digits. The called party parameter in SS7 MINT Gamma Signaling is represented as `F+C+PPP+CALLED NUMBER`, where `CALLED NUMBER` is the called number digits dialed and `F+C+PPP`

represents the MINT Gamma digits. CCS PM traps *only* on the CALLED NUMBER digits, *not* on the Gamma digits (F+C+PPP) that preface the called number digits in the IAM.

8.2.9.3 TCAP Limitations

- (1) In general, transactions that are initiated by craft test query functionality are not monitored, though transactions associated with the LASS Screen List Editing (SLE) DN Validation request utility (OP:LASSRQST) can be monitored.
- (2) A monitored TCAP message that is received on a PSU platform may differ in content at the MTP and SCCP layers than the actual message received on the SS7 link, though they are identical from a functional perspective. Because the PSU processes the MTP and SCCP layers of the message and passes a summary of this information to the SM along with the actual TCAP message content, the SM must then reconstruct the MTP and SCCP layers for messages that are being monitored. The specific scenario is related to a Called Party Address or a Calling Party Address which contains a point code format. Point codes can be encoded in two different formats:

Format 1

- Address Length
- Address Indicator
 - subsystem number present
 - point code present
 - no global title
 - route on point code/subsystem number
 - national standard
- Subsystem Number
- Point Code

Format 2

- Address Length
- Address Indicator
 - subsystem number present
 - point code not present
 - no global title
 - route on point code/subsystem number
 - national standard
- Subsystem Number
- no Point Code

For Format 2, because there is no point code present (though the address indicator states to route on point code), the Destination Point Code (DPC, for Called Party Address) or the Originating Point Code (OPC, for Calling Party Address) is used. Though Formats 1 and 2 are encoded differently, they are functionally identical and are routed in identical fashion by the network.

Because the PSU-to-SM interface does not distinguish between these two formats, messages are always reconstructed using Format 1.

- (3) If the DLN switches during a TCAP PM session, the PM recorder on the DLN terminates and the PM session data is lost.

8.2.10 Incompatibilities

No incompatibilities are associated with this feature.

8.2.11 Dependencies

No other features need to be installed or activated in order for this feature to work.

8.2.12 Isolation Constraints

No isolation constraints are associated with this feature.

8.2.13 Recent Change Provisioning

The service provider enables the CCS Protocol Monitor feature by populating the following fields in RC/V view 8.22, SECURED FEATURE UPGRADE:

FIELD	VALUES
FEATURE ID	260
MODULE	OFC
PASSWD	(Obtain from Lucent Technologies SFID Administrator)
ACTIVE	Y

8.2.14 Customer Premises Equipment (CPE)

Not applicable.

8.2.15 Maintenance Considerations

Not applicable.

8.2.16 Administration

8.2.16.1 Measurements

This feature does not impact measurements.

8.2.16.2 Billing

This feature does not impact billing.

8.3 DIAGNOSTIC COMMANDS

8.3.1 Manual Diagnostic (DGN) Commands

The manual diagnostic (DGN) commands are used for CNI ring node diagnostics. The DGN command has several formats, some of which are outlined in Table 8.3-1. In the DGN commands and in other messages used with the CNI, the term `nodexx=y` is used to identify either a ring peripheral control node (RPCN) or a link node (LN). It is necessary to insert the appropriate node type before using the commands from this manual. The direct link nodes (DLNs) are treated as LNs for diagnostics.

Table 8.3-1 CNI Diagnostic Message Input Variations

COMMAND	FUNCTION
DGN:nodexx=y	Runs all automatic phases on <code>nodexx=y</code> .
DGN:nodexx=y:PH a	Runs only the specified phase (a) on <code>nodexx=y</code> .
DGN:nodexx=y:PH a-b	Runs all automatic phases within the specified range (a through b) on <code>nodexx=y</code> .
DGN:nodexx=y;RPT n	Runs all automatic phases on <code>nodexx=y</code> and repeats execution n times, where $n \leq 255$.
DGN:nodexx=y;RAW	Runs all automatic phases on <code>nodexx=y</code> and prints the diagnostic results of every phase at the maintenance read-only printer (ROP).
DGN:nodexx=y;UCL	Runs all automatic phases on <code>nodexx=y</code> . Early terminations built into data tables are ignored.
DGN:nodexx=y;TLP *	Runs all automatic phases on <code>nodexx=y</code> and executes the trouble locating process at the conclusion of the diagnostics. This process prints at the maintenance ROP and CRT a list of possible faulty equipment.

8.3.2 Obtaining the Status of the CNI Ring

When performing the interprocess message switch (IMS) CNI ring node diagnostics, it may be necessary to obtain visual status of the signaling system, the CNI ring, or a particular node. One way of obtaining this status is the use of the OP input message. Figure 8.3-1 gives an example of the OP input commands and identifies the components of the output message. Table 8.3-2 lists the formats for most of the OP commands and the status information invoked by each command.

OP:RING INPUT COMMAND	OUTPUT RESPONSE
OP:RING	RING ACTIVE, NO ISO SEG ↑ — RING MAINTENANCE STATE
OP:RING,DETD	— RING MAINTENANCE STATE ↓ RING ACTIVE, NO ISO SEG GP 00 AAAA 01 02 30. . . . 31. . . . 32 AAAA. . . . ↑ — NODE MAJOR STATE
OP:RING,LN00=1	— NODE MAJOR STATE ↓ — NODE MINOR STATE: MAINTENANCE MODE ↓ LN00 1: MJ=ACT; NM=AUTO; RI=USBL; NP=USBL IN ACT SEG ↑ — NODE MINOR STATE: RING POSITION ↗ — NODE MINOR STATE: RI HARDWARE ↖ — NODE MINOR STATE: NP HARDWARE

Figure 8.3-1 OP:Ring Commands

The status of the IMS system may also be obtained by calling up the 118 display page from the master control center (MCC).

Table 8.3-2 Input (OP) Messages for Obtaining CNI Ring Status

INPUT MESSAGE	FUNCTION
OP:RING,nodexx=y	Provides status information for the specified node (RPCN, DLN or LN).
OP:RING,GRP xx	Provides status information for all nodes on a specified frame group (for example, 00 or 32).
OP:RING	Provides ring status.
OP:RING;SUM	Provides a summary of the CNI ring information.
OP:RING;DETD	Provides detailed status of the CNI ring.
OP:OOS	Provides status information of all out-of-service equipment.
OP:RING,nodexx=y;GEN	Requests generic information for the specified node (RPCN, DLN, or LN).

The ring maintenance state defines the overall operational state of the ring. The ring maintenance state may be one of the following:

- (1) **Ring Normal** - Two ring configuration with no isolated nodes.
- (2) **Ring Isolated** - The ring has an isolated segment with begin isolated segment (BISO) and end isolated segment (EISO) nodes.

- (3) **Ring Restoring** - The ring contains an isolated segment and the restoration activity is in progress.
- (4) **Ring Down** - The ring is unusable from the Administrative Module (AM); however, the ring nodes may be able to communicate among themselves.
- (5) **Ring Normal-Listen** - Ring is normal, but is in the listening mode.
- (6) **Ring Isolated-Listen** - Ring is isolated, but is in the listening mode.
- (7) **Ring Restoring-Listen** - Ring is restoring, but is in the listening mode.
- (8) **Ring Configuring-No BISO/EISO** - This is a transient state when ring is being configured.
- (9) **Ring Configuring-Isolated** - This is a transient state when ring is being configured with an isolated segment.

The `OP:RING, DETD` command gives the node major state in a single letter format. Upper case letters indicate the active portion of the ring. Lower case letters indicate the isolated portion of the ring. Table 8.3-3 gives definitions for the abbreviations of the single letter format.

Table 8.3-3 Major Node State Abbreviations

ACTIVE SEGMENT	STATUS	ISOLATED SEGMENT OR RINGDOWN
A	Active	--
S	Standby	s
B	Initializing	b
F	Offline	f
O	Out-of-Service	i
U	Unavailable	u
•	Unequipped	•

The node major state shows the overall status of a node during normal system operation. The major state is the same as the equipment configuration data (ECD) and is defined as follows:

- (1) **Active (ACT)** - The node is active and performing on-line functions.
- (2) **Standby (STBY)** - The node is an RPCN that is operating, but the ring configuration is not completed or the ring is down.
- (3) **Initializing (INT)** - This is a transient state used to restart nodes on the ring.
- (4) **Off-Line (OFL)** - The node is out of service and neither restore nor removal is permitted.
- (5) **Out of Service (OOS)** - The node is out of service and unavailable for normal use, but is available for maintenance and diagnostics.
- (6) **Grow (GROW)** - The node is physically being added or removed from the ring. This state is entered only by changing the equipment configuration data.
- (7) **Unequipped (UNEQ)** - The node is unequipped but an equipment configuration data record may exist.

The node minor state for the CNI ring position indicates the position of the node relative to the current configuration of the ring. These minor state indications are as follows:

- (1) **NORM or IN ACT SEG = Normal** - The node is included in the active ring and is not a BISO or EISO node.

- (2) **Begin isolated segment (BISO)** - The node is included in the active ring and forms the beginning of the isolated segment.
- (3) **End isolated segment (EISO)** - The node is included in the active ring and forms the end of the isolated segment.
- (4) **Isolated (ISO)** - This node is contained in the isolated segment of the ring.

The node minor state for the node processor hardware indicates the maintenance state of the hardware. The minor state values are as follows:

- (1) **Usable (USBL)** - The node processor is usable.
- (2) **Faulty (FLTY)** - The node processor is known to be or is suspected to be faulty.
- (3) **Untested (UNTSD)** - The condition of the node processor is unknown.

The node minor state for the ring interface hardware indicates whether a node can be included in the active ring. The ring interface hardware states are as follows:

- (1) **Usable (USBL)** - The ring interface hardware is usable.
- (2) **Quarantine usable (QUSBL)** - The ring interface hardware is partially usable. The node can be included in the active ring but must be in a quarantine (out-of-service) state.
- (3) **Faulty (FLTY)** - The ring interface hardware is faulty and the node must be isolated.

The node minor state for maintenance mode indicates whether the restoration of nodes will be attempted by the automatic ring recovery. The maintenance mode node minor state values are as follows:

- (1) **Automatic (AUTO)** - The node is under the automatic control of automatic ring recovery.
- (2) **Manual (MAN)** - The node is under manual control and only manual user activity can restore the node to service.

The CNI ring diagnostic routines are divided into phases and described in the following tables:

- Table 8.3-4 : IRN2 Ring Peripheral Controller Node Diagnostic Phases
- Table 8.3-5 : IRN2 IMS User Node Diagnostic Phases
- Table 8.3-6 : IRN2 Direct Link Node Diagnostic Phases
- Table 8.3-7 : IRN2 Link Node Diagnostic Phases

The phases are arranged to test functionally related groups of hardware. Each phase may test all or part of a single circuit pack (CP) hardware, or it may test all or part of several CPs. Each ring node is diagnosed by its own set of diagnostic phases.

These terms are used in the diagnostic phase tables:

Begin Isolation (BISO) Controller Unit (CU)	Node Processor (NP) Memory Data Link (MDL)

Dual Serial Channel (DSCH) Dual Duplex Serial Bus Selector (DSBS) Equipment Configuration Data Base (ECD)	Main Store Controller (MASC) Maintenance Read-Only Printer (MROP) Master Control Center (MCC) Ring Access Circuit Bus 0 (RAC-0) Ring Access Circuit Bus 1 (RAC 1) X.25 Protocol Controller (X.25)

Table 8.3-4 IRN2 Ring Peripheral Controller Node Diagnostic Phases

PHASE	PHASE DESCRIPTION
01	Tests that a message can be relayed from the BISO node to the EISO node via the isolated segment over ring 0. Phase 1 also tests that any interframe buffers and all IRN boards in the isolated segment are equipped in accordance with ECD data, and that any interframe buffers in the isolated segment exhibit the proper data storage capacity.
02	Tests that a message can be relayed from the EISO node to the BISO node via the isolated segment over ring 1. Phase 2 also tests that any interframe buffers and all IRN boards in the isolated segment are equipped in accordance with ECD data, and that any interframe buffers in the isolated segment exhibit the proper data storage capacity.
10	Tests the interface between the Dual Serial Channel (DSCH) and the DDSBS.
11	Tests the interface between the DBSBS and the 3BI.
12	Verifies that RAC0 can detect bad parity in a ring message.
13	Verifies that RAC1 can detect bad parity in a ring message.
14	Off-line CU to DSBS tests (Demand phase only).
20	Tests the NP RAM memory and the NP parity checker and generator circuitry.
30	Tests part of both RAC circuits, and the RAC to NP interface. Partially tests interface between both RACs and the ring bus.
32	Verifies that RAC0 can detect bad parity in a ring message.
33	Verifies that RAC1 can detect bad parity in a ring message.
39	Verifies the ability of the node to read, write, and propagate a maximum-length long message. This is a demand phase, and is provided only in a transition load. In the long message load, this phase is phase 0.

Table 8.3-5 IRN2 IMS User Node Diagnostic Phases

PHASE	PHASE DESCRIPTION
01	Tests that each node in the isolated segment is able to set and clear its data selector via hardware commands at RAC0. Phase 1 also tests that a message can be relayed from the BISO node to the EISO node via the isolated segment over ring 0, and that any interframe buffers in the isolated segment are equipped in accordance with ECD data and exhibit the proper data storage capacity.
02	Tests that each node in the isolated segment is able to set and clear its data selector via hardware commands at RAC1. Phase 2 also tests that a message can be relayed from the EISO node to the BISO node via the isolated segment over ring 1, and that any interframe buffers in the isolated segment are equipped in accordance with ECD data and exhibit the proper data storage capacity.
10	Tests part of both RACs, the RAC to NP interface, and the interface between both RACs and the ring bus. Checks the capacity of the interframe buffers associated with the node under test.
12	Verifies that RAC0 can detect bad parity in a ring message.
13	Verifies that RAC1 can detect bad parity in ring message.
20	Tests the NP RAM memory and the NP parity checker and generator circuitry.

Table 8.3-6 IRN2 Direct Link Node Diagnostic Phases

PHASE	PHASE DESCRIPTION
01	Tests that each node in the isolated segment is able to set and clear its data selector via hardware commands at RAC0. Phase 1 also tests that a message can be relayed from the BISO node to the EISO node via the isolated segment over ring 0, and that any interframe buffers in the isolated segment are equipped in accordance with ECD data and exhibit the proper data storage capacity.
02	Tests that each node in the isolated segment is able to set and clear its data selector via hardware commands at RAC1. Phase 2 also tests that a message can be relayed from the EISO node to the BISO node via the isolated segment over ring 1, and that any interframe buffers in the isolated segment are equipped in accordance with ECD data and exhibit the proper data storage capacity.
10	Tests part of both RACs, the RAC to IRN2 interface, and the interface between both RACs and the ring bus.

12	This phase verifies that RAC0 can detect bad parity in a ring message.
13	This phase verifies that RAC1 can detect bad parity in a ring message.
20	Tests the IRN2 RAM memory and the parity checker and generator circuitry.
30	Tests interface between the DSCH and the DDSBS.
31	Tests interface between the DDSBS and the 3BI.
32	Tests ability of NP to go "insane" and set the "Interrupt Request Flag" when the 3BI has an error.
33	Tests the interface between 3BI and the NP.
34	Off-line CU to DDSBS tests (Demand phase only).
35	Cooperates with the 3B20D/3B21D driver to test the DMA capability via the 3BI.
40	Tests the shared static memory in the AP30 from the IRN2 side.
41	Tests the shared static memory from the AP30 side, the local parity error snapshot register, and the main 16 Megabytes of DRAM on the AP30.
42	Tests DMA capability via the 3BI. The DMA is from the 3B20D/3B21D to/from the AP Dual Port Memory (DPM).
43	Tests the four D-channel data links on the AP30 (demand-only).

Table 8.3-7 IRN2 Link Node Diagnostic Phases

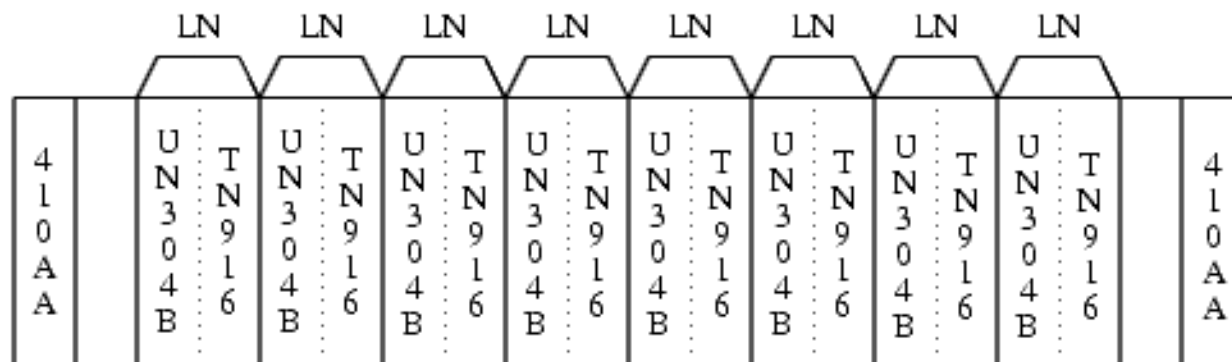
PHASE	PHASE DESCRIPTION
01	Tests that each node in the isolated segment is able to set and clear its data selector via hardware commands at RAC0. Phase 1 also tests that a message can be relayed from the BISO node to the EISO node via the isolated segment over ring 0, and that any interframe buffers in the isolated segment are equipped in accordance with ECD data and exhibit the proper data storage capacity.
02	Tests that each node in the isolated segment is able to set and clear its data selector via hardware commands at RAC1. Phase 2 also tests that a message can be relayed from the EISO node to the BISO node via the isolated segment over ring 1, and that any interframe buffers in the isolated segment are equipped in accordance with ECD data and exhibit the proper data storage capacity.
10	Tests part of both RACs, the RAC to the NP interface, and the interface between both RACs and the ring bus. Checks the capacity of the interframe buffers associated with the node under test.
12	This phase verifies that RAC0 can detect bad parity in a ring message.
13	This phase verifies that RAC1 can detect bad parity in a ring message.
20	Tests the NP RAM memory and the NP parity checker and generator circuitry.
39	Verifies the ability of the node to read, write, and propagate a maximum-length long message (demand only phases for transition load).
40	Tests hardware in the LI board or the LI-NP interface.
41	This phase tests the sanity of the microprocessor and the ROM.
47	Tests the 2.4 and the 4.8 data service units, along with their respective VFLA or DSA units. CCS7 will ATP by default.
48	This phase insures that the firmware and the hardware on the LI board will function as a whole.

8.3.3 Manual Trouble Location Circuit Pack List

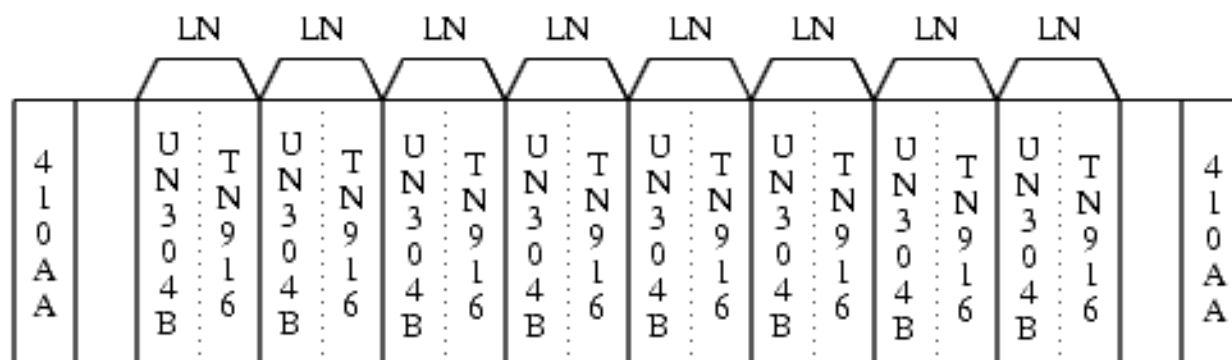
Each piece of hardware that is tested by a diagnostic phase has suspected probable faulty circuit packs. If the diagnostic results returned from ring diagnostics is STF (some tests failed), the following tables provide a list of possible circuit packs that are associated with each phase:

- Table 8.3-8 : IRN2 Ring Peripheral Controller Node Trouble Location Circuit Pack List
- Table 8.3-9 : IRN2 Link Node Trouble Location Circuit Pack List
- Table 8.3-10 : IRN2 Direct Link Node 30 (DLN30) Trouble Location Circuit Pack List

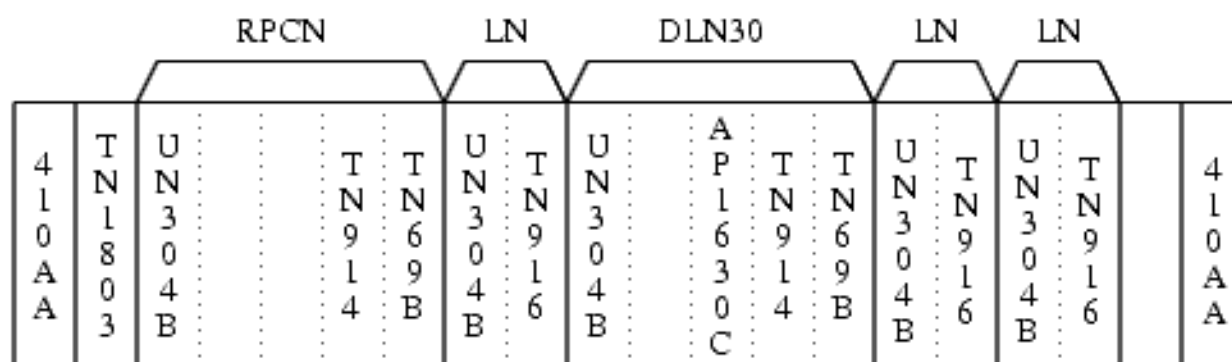
Examples of possible circuit pack assignments in the CNI shelves used in the 5ESS®-2000 switch arrangement are shown in Figure 8.3-2 (for IRN2).



SHELF J3F011GC



SHELF J3F011GC



SHELF J3F011GD

Figure 8.3-2 IRN2 CNI Shelves Circuit Pack Arrangement

Table 8.3-8 IRN2 Ring Peripheral Controller Node Trouble Location Circuit Pack List

DIAGNOSTIC PHASE		PROBABLE/SUSPECTED FAULTY	UNIT NAME
PHASE	TABLE		

PACK			
01	RPC01.1	UN304B	IRN2
		TN1803	IFB
		Ring bus cable	RNF/C
02	RPC02.1	Same as Phase 01	Same as Phase 01
10	RPC10.1	TN69B	DDSBS
		UN09 (on 3B)	DSCH
11	RPC11.1	TN914	3BI
		TN69B	DDSBS
12	RPC12.1	TN914	3BI
		UN304B	IRN2
13	RPC13.1	TN914	3BI
		UN304B	IRN2
14	RPC14.1	TN69B	DDSBS
			(Demand only phase)
		UN09 (on 3B)	Off-line DSCH
20	RPCI20.1	UN304B	IRN2
21	RPCI21.1	UN304B	IRN2
30	RPCI30.1	UN304B	IRN2
32	RPC32.1	UN304B	IRN2
		TN1803	IFB
33	RPC33.1	Same as Phase 32	Same as Phase 32

Table 8.3-9 IRN2 Link Node Trouble Location Circuit Pack List

DIAGNOSTIC PHASE		PROBABLE/SUSPECTED FAULTY PACK	UNIT NAME
PHASE	TABLE		
01	IUN01.1	UN304B	IRN2
			IFB
		Ring Bus Cable	RNF/C
02	IUN02.1	Same as Phase 01	Same as Phase 01
10	IUN10.1	UN304B	IRN2
12	IUN12.1	UN304B	IRN2
			IFB
13		Same as Phase 12	Same as Phase 12
20	IUN20.1	UN304B	IRN2
21	IUN21.1	UN304B	IRN2
39	IUN39.1	UN304B	IRN2
40	cBph0.40.1	TN916	LI-NE
		UN304B	IRN2
41	cBph1.41.1	Same as Phase 40	Same as Phase 40
47	cBph7.47.1	Will ATP by default.	
48	cBph8.48.1	TF9	Facility Int.
		Z2566L1A/2 ^a	Data Sets
		TN916	LI-NE
		Link Cabling	

Notes:

a. Phase 48 - Test 47 will fail if Z2566L1A/2 is in Local Loop (LL).

Table 8.3-10 IRN2 Direct Link Node 30 (DLN30) Trouble Location Circuit Pack List

DIAGNOSTIC PHASE		PROBABLE/SUSPECTED FAULTY PACK	UNIT NAME
PHASE	TABLE		
01	IUN01.1	UN304B	IRN2
		TN1803	IFB-4K/8
		Ring Bus Cable	RNF/C
02	IUN02.1	Same as Phase 01	Same as Phase 01
10	IUN10.1	UN304B	IRN2
12	IUN12.1	UN304B	IRN2
		TN1803	IFB-4K/8
13	IUN13.1	Same as Phase 12	Same as Phase 12
20	IUN20.1	UN304B	IRN2
30	IUN30.1	TN69B	DDSBS
		UN09 (on 3B)	DSCH
31	IUN31.1	TN914	3BI
		TN69B	DDSBS
32	IUN32.1	TN914	3BI
		UN304B	IRN2
33	IUN33.1	TN914	3BI

		UN304B	IRN2
34	IUN34.1	TN69B	DDSBS (Demand only phase)
		UN09 (on 3B)	Off-line DSCH
35	IUN35.1	Same as Phase 33	Same as Phase 33
40	AP68.40.1	TN1630C	AP30
41	LI4E.41.1	TN1630C	AP30
42	AP68.42.1	TN1630C	AP30
43	LI4E.43.1	TN1630C	AP30 (Demand only)

8.4 TROUBLE INDICATIONS AND ANALYSIS

The following tables provide information for analyzing alarm conditions and determining what troubles are indicated.

- Table 8.4-1 : CNI/IMS Trouble Indicators and Analysis MROP Output Messages
- Table 8.4-2 : CNI/IMS Trouble Indicators and Analysis Visual Alarms At Maintenance CRT
- Table 8.4-3 : CNI/IMS Trouble Indicators and Analysis Visual Alarms At Ring Node Cabinet
- Table 8.4-4 : CNI/IMS Trouble Indicators and Analysis Audible Alarms

Table 8.4-1 contains the trouble indications that are contained in output messages at the maintenance receive-only printer (MROP). Table 8.4-2 contains the trouble conditions indicated by visual alarms observed on the MCC, and Table 8.4-3 contains the visual alarms observed at the light emitting diodes (LEDs) at the CNI ring cabinet. The trouble conditions indicated by the office audible alarms are contained in Table 8.4-4.

Table 8.4-1 CNI/IMS Trouble Indicators and Analysis MROP Output Messages

ALARM INDICATION		AFFECTED EQUIPMENT		SERVICE
MESSAGE	ALARM	RING	OTHER	AFFECTED
ALM BATTERY ALM	Major		Power	No
CO BATTERY DISCH	Major		Power	No
LOST PROTECTED AC	Major		Power	Yes/No ^a
	Minor		3B20D	
POWER FAILURE ON	Major		Power	Yes/No ^a
	Minor		3B20D	
POWER RM ALM	Major	RPCN	Power	Yes
	Minor	IUN	3B20D	
REPT DB INIT	Major		3B20D	Yes
REPT ERROR	Major	RPCN	3B20D	Yes/No ^a
		IUN		
REPT IMSDRV FLT	Minor	RPCN		Yes/No ^a
		IUN		
REPT IMSDRV INIT	Major	RPCN	3B20D	Yes
	Minor	IUN		
REPT IUN	Minor	IUN		No
REPT RING CFR	Minor	RPCN		Yes/No ^a
		IUN		
REPT RING GROWTH	Minor	RPCN		No
		IUN		
REPT RING INIT	Major	RPCN	3B20D	Yes
		IUN		
REPT RING TRANSPORT ERR	Minor	RPCN		No
		IUN		
REPT TOKEN TRACK		RPCN		Yes
		IUN		
RMV IUN	Minor	IUN		No
RMV RPCN	Major	RPCN		Yes/No ^a
	Minor			
Notes:				
a. Service may be affected depending on the status of the components.				

Table 8.4-2 CNI/IMS Trouble Indicators and Analysis Visual Alarms At Maintenance CRT

ALARM INDICATION AT MCRT	AFFECTED EQUIPMENT		SERVICE AFFECTED
	RING	OTHER	
MAJOR	RPCN	Power	Yes
	IUN	3B20D	

MINOR	RPCN IUN	Power 3B20D	No
BLDG PWR	RPCN IUN	3B20D	Yes/No ^a
SYS EMER		Power 3B20D	Yes
OTHER			
Notes:			
a. Service may be affected depending on the status of the components.			

Table 8.4-3 CNI/IMS Trouble Indicators and Analysis Visual Alarms At Ring Node Cabinet

ALARM INDICATION AT RING NODE CABINET	AFFECTED EQUIPMENT		SERVICE AFFECTED
	RING	OTHER	
RING QUARANTINE	RPCN IUN		Yes/No ^a
NO TOKEN	RPCN IUN		Yes
ALM	RPCN IUN		No
POWER ALM		Power	No
DIAG FAIL	RAP		Yes/No ^a
ERROR	AP		Yes/No ^a
Notes:			
a. Service may be affected depending on the status of the components.			

Table 8.4-4 CNI/IMS Trouble Indicators and Analysis Audible Alarms

ALARM INDICATION IN THE OFFICE	AFFECTED EQUIPMENT		SERVICE AFFECTED
	RING	OTHER	
MAJOR	RPCN IUN	Power 3B20D	Yes/No ^a
MINOR	RPCN IUN	Power 3B20D	No
ALM BAT SUPPLY		Power	No
POWER PL MAJOR		Power 3B20D	Yes/No ^a
Notes:			
a. Service may be affected depending on the status of the components.			

8.5 TIPS FOR CNI TROUBLESHOOTING

This section provides switch personnel in the 5ESS®-2000 switch office with tips for troubleshooting the common network interface (CNI) ring through ring recovery procedures.

8.5.1 Ring Fault Recovery

8.5.1.1 Subsystems

The CNI ring fault recovery is accomplished by the *Error Analysis and Recovery (EAR)* and the *Automatic Ring Recovery (ARR)* subsystems working together. Also see "Safety Net for CNI Ring Recovery Feature," Section 8.6.

8.5.1.2 Error Analysis and Recovery Subsystem (EAR)

This subsystem provides automatic and rapid recovery from faults that it detects. Its centralized control in the AM provides for error detection and partial recovery in the ring nodes. The results of this subsystem action may be quarantined nodes and isolated ring segments containing faulty nodes.

8.5.1.3 Error Analysis and Recovery System Levels of Ring Recovery

The EAR system attempts ring recovery through a series of ring reconfiguration levels, as follows:

- Level 0:** The EAR first attempts to establish the original ring configuration. The alternative is large isolation.
- Level 1:** The next configuration level is an attempt to establish a configuration based on detected errors. This leaves a portion of the ring isolated.
- Level 2:** This level expands the isolated by the following:
- One node
 - Any faulty node.
- Level 3:** Establish the largest ring possible with the available segment components.
- Level 4:** Retry level 3.
- Level 5:** Place entire CNI ring in down state.

8.5.1.4 Automatic Ring Recovery

The ARR is a subsystem used to defer ring fault recovery. It automatically diagnoses and restores nodes that have been removed or isolated by the EAR subsystem.

8.5.1.5 Automatic Ring Recovery Node Restoral Priorities

The restoration of out-of-service (OOS) nodes by the ARR subsystem is performed by grouping the nodes eligible to be restored. Following is the order of restoration:

- (1) Nodes serving as begin isolation (BISO) or end isolation (EISO) node.
- (2) Nodes with faulty interfaces (also includes nodes within an isolated segment and in an untested state).

- (3) Nodes with faulty interfaces (if critical node restoration is used).
- (4) Ring peripheral controllers (RPCs) eligible for unconditional restoration.
- (5) USER critical node high priority (if critical, node restoration feature is used).
- (6) RPCs eligible for conditional restoration.
- (7) USER critical node low priority (if critical, node restoration feature is used).
- (8) IUNs eligible for unconditional restoration.
- (9) IUNs eligible for conditional restoration.

8.5.1.6 Manual Input Controls

When equipment is automatically removed from service because of a fault, manual action should not be attempted until the automatic ring recovery system has attempted to restore the equipment and marked it for manual action. When manual restoration or diagnostics are desired, the automatic ring recovery system should be inhibited to avoid conflicting with automatic requests. Table 8.5-1 contains the manual input control messages along with their actions.

Table 8.5-1 Manual Diagnostics and Restoral Requests

COMMAND ^a	ACTION
INH:DMQ:SRC=ARR	Conditional restorals are inhibited
OP:DMQ	View active and queued restoral requests
STP:DMQ:LNXX=Y	Active or queued Link Node restoral requests are stopped
STP:DMQ:RPCNXX=Y	Active and queued RPCN restoral requests are stopped
RST:LNXX=Y	Manual request for Link Node restoral
RST:RPCNXX=Y	Manual request for Ring Peripheral Controller Node restoral
DGN:LNXX=Y	Manual request for Link Node diagnostics
DGN:RPCN=Y	Manual request for Ring Peripheral Controller Node diagnostics
ALW:DMQ:SRC=ARR	Allow Automatic Ring Recovery to return to normal operation
INH:DMQ:ARC=CNR	Inhibit the Critical Node Restoral feature (if implemented)
ALW:DMQ:SRC=CNR	Allows the Critical Node Restoral feature to function
Notes:	
a. Diagnostics and restoral requests may be performed with a poke command on MCC Page 118.	

8.5.2 Performing Manual Diagnostics On A Node

8.5.2.1 Sequence of Procedures

Following is a sequence of procedures for performing manual diagnostics on a node:

- (1) If the node major state is OOS and its minor state for maintenance mode is AUTO, inhibit the automatic ring recovery and stop any restorations initiated by the automatic ring recovery (see Table 8.5-2).
- (2) If the node is an LN with a major state of ACT, input the following message to change the signaling link major state to manual out-of-service.

 — CHG:SLK=XX-Y:MOOS (Where XX is the group number and Y is the member number).
- (3) Diagnose the node using the DGN:NOSEX=Y command where XX=LN, DLN, or RPCN. Alternatively, the RST:RPCNXX=Y or RST:LNXX=Y commands can be used to diagnose the node. If diagnostics produce all tests passed, restore the node to service.

- (4) Resolve any failing diagnostics until all tests pass. Replace faulty circuit packs using the circuit pack replacement procedures. When all tests passed is achieved, go to Step 7.
- (5) If the diagnostics produced a conditional all tests passed, determine the reason for the conditional status. If the reason is "the node was not singly isolated," perform the following:
 - (a) Unconditionally restore the node (Step 7).
 - (b) Conditionally restore the adjacent nodes.
 - (c) After the adjacent nodes are restored, conditionally restore the original node that was unconditionally restored in Step 5a. Go to Step 8.
- (6) If diagnostics results in a "no test run" or "aborted test," determine the reason. Use the `OP:RING, RPCNXX=Y` or `OP:RING, LNXX=Y` command to help determine the cause. Go back to Step 3 when the problem is cleared.
- (7) If the `DGN` command was used, it is necessary to restore the node unconditionally with `RST:RPCNXX=Y`, `RST:LNXX=Y`, or a poke on the 118 Page. A node should not be restored unconditionally unless one of the following conditions is met:
 - A complete diagnostics has produced an ATP response.
 - A complete diagnostics has produced a conditional all tests passed response and the ring interface and node processor minor states are both usable (USBL).
- (8) If the node is an LN, input the following message to change the signaling link minor state to in-service:
`CHG:SLK=XX-Y:IS.`

8.5.2.2 Resolving Diagnostic Failures

When the results of a diagnostic in some tests failed, circuit packs should be replaced using the manual trouble location circuit pack list for appropriate node types. Before physically removing any circuit pack, it is necessary to ensure that the faulty node has the proper major and minor states. If the node has not been removed from service, it should be removed with the `RMV:LNXX=Y` or `RMV:RPCNXX=Y` command. The node should then be isolated from the active ring with the `CFR:RING, LNXX=Y:EXCLUDE` or `CFR:RING, RPCNXX=Y:EXCLUDE` command. There are certain packs in each of the nodes which have light emitting diode (LED) indicators on the front of the packs. These are summarized in Table 8.5-2.

Replace circuit packs using the circuit pack removal procedure.

8.5.3 Circuit Pack Removal

Part of the CNI troubleshooting may require the replacement of circuit packs. This requires the isolation of the circuit pack from the active ring. To avoid unnecessarily large isolated segments of the ring, the trouble conditions requiring isolation should be cleared promptly. However, precautions must be taken when removing defective circuit packs to avoid damages to the active part of the ring. Some of these precautions are as follows:

- Visual LED indicators should be inspected for illumination.
- The node in which the circuit pack is located should be out of service and isolated before any circuit pack is replaced.

- If the node is out of service and isolated, the RQ and NT LEDs should be lighted.

Table 8.5-2 provides the list of LEDs that should be illuminated when replacing the various circuit packs.

Table 8.5-2 LED Illumination for Circuit Pack Removal

CIRCUIT PACK TO BE REPLACED	LEDS TO BE ILLUMINATED
UN123B (RI0)	NT LED on UN123B
UN123B (RI1)	NT LED on UN123B
TN922 (NP)	RQ LED on TN922 or TN LED on UN123B
TN916 (II)	RQ LED on TN916 or TN LED on UN123B
TN915 (PIFB)	NT LED on UN123B or NT LED on UN123B of the neighbor node that also contains a TN915
TN918 (IFB)	NT LED on UN123B or NT LED on UN123B of the neighbor node that also contains a TN918
TN914 (3BI)	RQ LED on TN922 or NT LED on UN123B
TN69B (DDSBS)	RQ LED on TN922 or NT LED on UN123B
495FA (Power)	NT LED on UN123B of adjacent node and NT LED on UN123 of center node (for 3 node LN shelf)

8.5.4 Diagnostic Failures Not Resolved By Replacing Circuit Packs

If circuit pack replacement does not resolve a diagnostic failure, other areas must be investigated.

- (1) The diagnostic that has failed should be investigated to determine what hardware is tested.
- (2) It is possible that the trouble could be located in a neighboring node.
- (3) A phase 1 failure may give a false diagnostic failure of an interframe buffer (IFB) or ring interface circuitry in the BISO or EISO node. This occurs when the phase 1 initiates a test to determine if a message can be relayed from the BISO node to the EISO node through the node that is being diagnosed.
- (4) Phase 1 checks the ring capacity against HV values. An incorrect HV value in the equipment configuration data (ECD) for the nodes under test or either of the adjacent nodes can cause phase 1 or phase 2 failures. The test is illustrated in Figure 8.5-1.

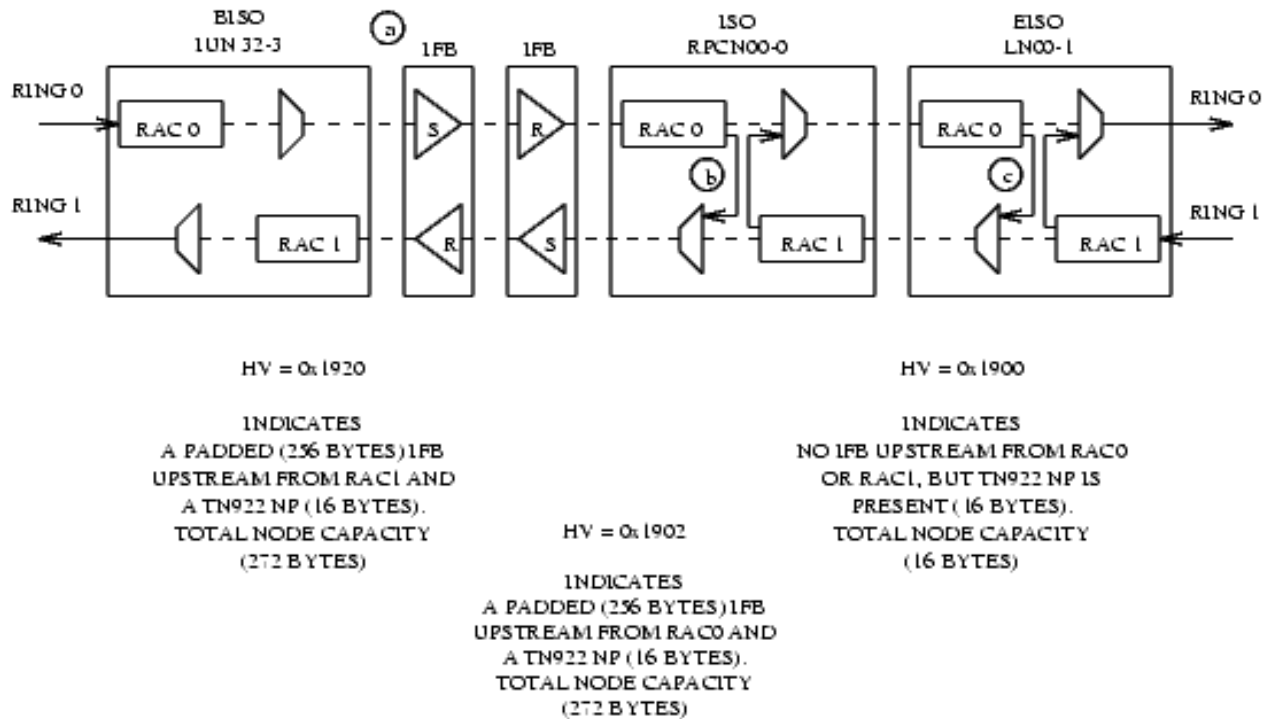


Figure 8.5-1 Checking the Ring Capacity Against HV Values

- (a) The BISO sends a byte pattern over ring 0 to the isolated node.
 - (b) At the RPCN, the byte pattern is looped back to the BISO where the number of bytes is measured against the expected capacity determined by the ECD.
 - (c) After clearing the data selector at the RPCN, the ring capacity test is again run to test the capacity all the way to the EISO and back.
- (5) In the event of a phase 1 diagnostic failure, run phase 2 to determine if there is any faulty hardware. Phase 2 is the same as phase 1, but the tests are run from the EISO instead of the BISO.
 - (6) Check the ECD maintenance value in the unit control block (UCB) form for each of the nodes. This maintenance value (UCB 27 - MV value) determines which type of node diagnostics to run. If the value is incorrect, the LN diagnostics may try to run on a DLN.
 - (7) If necessary, check the interframe buffering, cables, backplane, pins, or wiring.

8.5.5 Ring Node Is Out Of Service, And Automatic Ring Recovery Fails

When the fault recovery software removes a node from service and places it in the OOS-NORMAL state, the ARR attempts to diagnose and restore the node to service. If the ARR fails, the node is marked for manual action and placed in the ring maintenance state. Standard diagnostic procedures should be used for running diagnostics on the OOS node.

If the node remains in the OOS-NORMAL state after the following:

- (1) Running diagnostics

- (2) Resolving failures
- (3) Attempting to restore node to service.

Replace circuit packs in the following order:

- (1) NP - link interface
- (2) RI0 - ring interface 0
- (3) RI1 - ring interface 1.

CAUTION: Before replacing any of these packs, the node must be in the correct maintenance state.

If the replacement of these do not resolve the node problem, check for the following:

- (1) Shorts
- (2) Bent or broken pins
- (3) Cabling faults.

If none of these resolve the problem, perform diagnostics and circuit pack replacement on the adjacent nodes using standard procedures.

8.5.6 Automatic Ring Recovery Cannot Restore An Isolated Node

8.5.6.1 Standard Diagnostic Procedures

When the fault recovery software has removed a node from service and isolated it after an equipment malfunction, the AUTOMATIC RING RECOVERY subsystem attempts to diagnose and restore the node to service. If all tests in the diagnostics pass, but the node cannot be restored to service, the node is marked for manual action.

Diagnose the node using standard diagnostic procedures. If the node cannot be restored:

- (1) In a small ring -
 - (a) Diagnose the BISO node with the configuration fault recovery (CFR) command.
- (2) In a larger ring -
 - (a) Remove the BISO node from service.
 - (b) Diagnose the BISO node.
- (3) Diagnose the EISO node.
- (4) Replace circuit packs
 - (a) Ring interface 0 (RI0)
 - (b) Ring interface (RI1)

- (c) Interframe buffer or padded interframe buffer (PIFB)
- (d) Node processor (NP)
- (e) Link interface (LI)
- (f) Perform conditional restoration.

8.5.6.2 Precautions for Ring Hardware Troubleshooting

Certain precautions should be taken when troubleshooting the CNI ring hardware.

- DO NOT:** Do unconditional restoration on an isolated node unless it is certain that there are no faults existing in the node. If a node or a group of nodes were isolated due to a ring event, diagnostic phases 1 and 2 must be run. Otherwise, packs could be uninitialized and cause blockage.
- DO NOT:** Leave the automatic ring recovery or critical node restoration inhibited when the system is unattended.
- DO NOT:** Leave nodes out of service unnecessarily.
- DO:** When analyzing ring transport errors, be aware of the real-time clock that prints out on these messages to determine the order of the messages. These messages may be delayed when printed out to the receive-only printer.
- DO:** When troubleshooting a ring related problem, frequent use of the `OP:RING:DETD` command to record overall ring status can be beneficial later for study.
- DO:** Save the `RPTERR0` and `RPTERR1` log files in the `/log/log` if a problem is likely to be escalated.

8.6 SAFETY NET FOR CNI RING RECOVERY

8.6.1 Description

The Common Network Interface (CNI) provides ring fault recovery and diagnostic software, called Error Analysis and Recovery (EAR), that automatically identifies, isolates and diagnoses faulty ring hardware. Most ring transport problems caused by faulty hardware are identified and removed with minimal service disruption. The *Safety Net for CNI Ring Recovery* feature (96-CP-3101) identifies intermittent ring failures not found by existing EAR diagnostic software on 5ESS®-2000 switches equipped with CNI.

This feature is not secured and does not require a right-to-use (RTU) fee.

8.6.2 Cross References

- Feature number: 96-CP-3101
- Bellcore specifications: N/A

8.6.3 Availability

The *Safety Net for CNI Ring Recovery* feature is available as part of the 5E11 software release.

8.6.4 Feature Environment

This feature is provided on a per-office basis.

8.6.5 Feature Operation

The *Safety Net for CNI Ring Recovery* feature assumes the existence of only one intermittent ring node or inter-frame buffer hardware failure on the ring. The feature will isolate one node at a time until a stable ring configuration is found. If a ring failure occurs when a particular node is isolated, the feature assumes that the currently isolated node is not the problem and identifies and isolates another node and restores the previously isolated node. The feature uses certain ring EAR history data including the history of nodes isolated/restored to guide the choice of a node to be isolated.

If this strategy fails or results in "thrashing" (repeated but unsuccessful attempts at recovery) because of multiple failures or other reasons, the system will escalate into the half-ring mode, where one half of the ring is isolated in an attempt to reach a stable configuration. If another failure occurs, the system will then switch the active half-ring and the isolated half-ring.

If the half-ring strategy also fails, the *Safety Net for CNI Ring Recovery* feature will request a full processor initialization (FPI) or a boot similar to the action that would be taken by the ring EAR fault recovery software.

8.6.6 User Operation

8.6.6.1 For Subscribers

No subscriber action is associated with this feature.

8.6.6.2 For Switch Personnel

The *Safety Net for CNI Ring Recovery* feature provides several new input messages that are detailed in the 235-600-700, *Input Messages Manual*. A list of the new messages along with a brief description follows:

- `EXC:RTRACK` - permits manual entry into ring tracker.
- `STOP:RTRACK` - allows exit from ring tracker mode.
- `OP:RTRACK` - obtains history of node isolations.
- `INH:RTRACK` - inhibits entry into ring tracker mode.
- `ALW:RTRACK` - removes ring tracker from inhibit mode

8.6.7 Engineering

8.6.7.1 Hardware Resources

This feature requires no new hardware.

8.6.7.2 Software Resources

This feature requires no new software resources.

8.6.7.3 Transition Considerations

There are no transition considerations associated with this feature.

8.6.8 Interactions and Limitations

This feature normally finds only single intermittent ring hardware failures; it may not locate multiple failures. The half-ring strategy may stabilize the ring if the multiple failures are contained within the half-ring under test.

Only those ring transport errors currently handled by the EAR are detected by this feature.

8.6.9 Incompatibilities

This feature has no incompatibilities.

8.6.10 Dependencies

This feature has no dependencies.

8.6.11 Isolation Constraints

This feature has no isolation constraints

8.6.12 Feature Implementation

8.6.12.1 Office Data Administration (ODA) Provisioning

No ODA provisioning is required for this feature.

8.6.12.2 Recent Change Provisioning

No Recent Change provisioning is required for this feature.

8.6.13 Maintenance Considerations

The *Safety Net for CNI Ring Recovery* feature introduces several new output messages for message ID REPT:RING-CFR. Detailed information can be found in the 235-600-750, *Output Messages Manual*; however, a brief description along with examples of the new messages follow:

- This report is issued whenever the ring tracker mode requests isolation of node "a" while attempting to establish a service-providing ring.

```
CNI REPT RING CFR
ISOLATION OF a REQUESTED BY RTRACK
f f f f (g)
```

- This report is generated when the ring tracker mode requests a half ring boot.

```
CNI REPT RING CFR
HALF RING BOOT REQUESTED BY RTRACK
f f f f (g)
```

- This report is produced once every 15 minutes when the ring tracker mode is active and available to respond to ring failures.

```
CNI REPT RING CFR
RTRACK ATTEMPTING TO LOCATE INTERMITTENT CNI HARDWARE FAULT
f f f f (g)
```

- When ring tracker mode is active, this report is issued along with the previous message if the current ring configuration has been stable longer than the ring tracker confidence interval.

```
CNI REPT RING CFR
RTRACK CONFIDENCE INTERVAL OF r HRS s MINS REACHED WITH
CURRENT ISOLATED NODE(S)
(g)
```

- This report is issued when the ring tracker mode is exited.

```
CNI REPT RING CFR
RTRACK EXITING DUE TO MANUAL ACTION REQUEST
f f f f (g)
```

- This report is generated every 15 minutes when entry into the ring tracker mode is inhibited.

```
CNI REPT RING CFR
RTRACK MANUALLY INHIBITED
(g)
```

- This report is produced when entry into the ring tracker mode has been moved from the inhibit state.

```
CNI REPT RING CFR
RTRACK ALLOWED
(g)
```

8.6.14 Administration

8.6.14.1 Measurements

This feature requires no new measurements.

8.6.14.2 Billing

This feature does not affect billing.

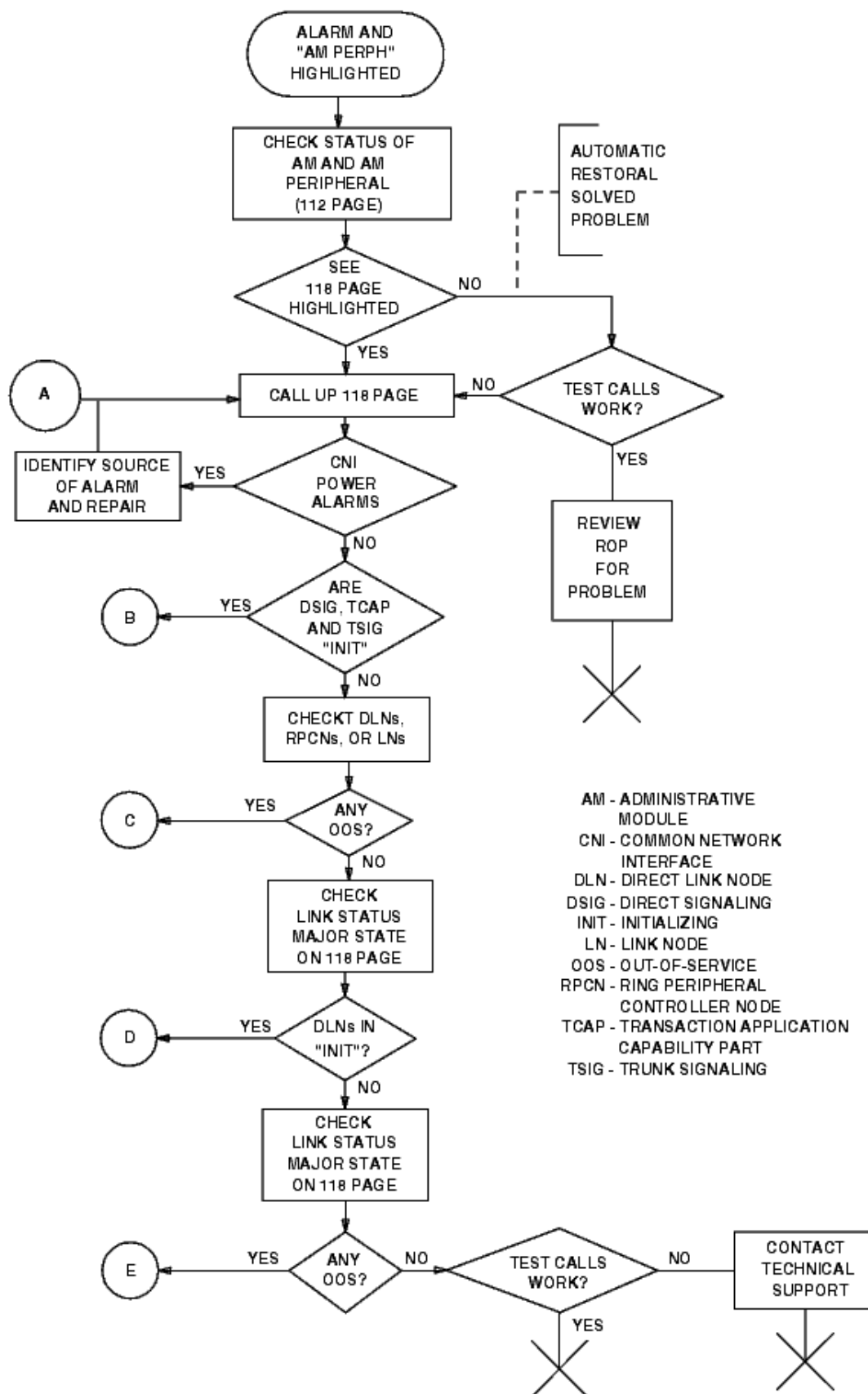
8.7 CCS NETWORK PROBLEMS

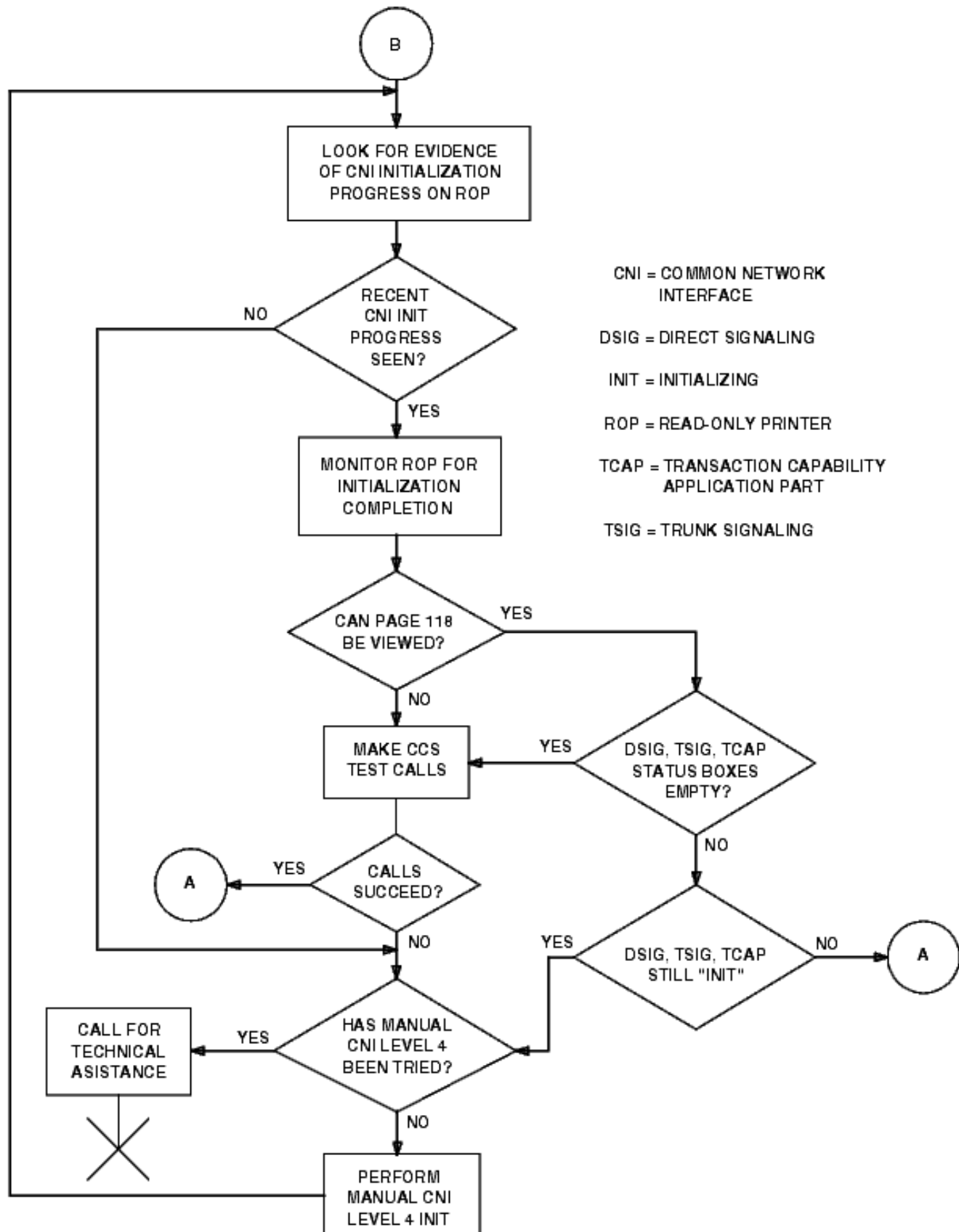
8.7.1 CCS Network Problems Introduction

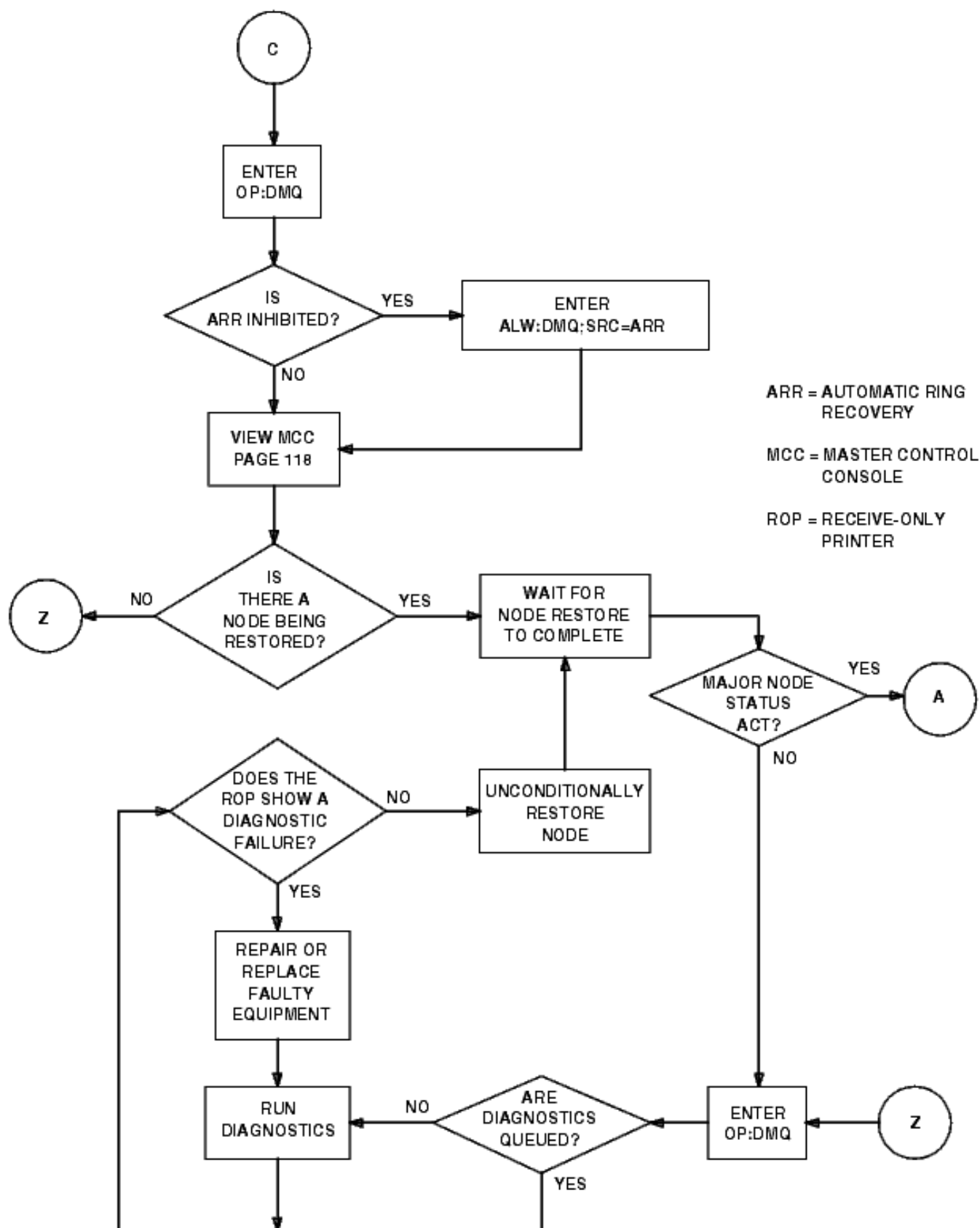
This section is intended to provide the switch office personnel with some general procedures for determining the cause of service loss due to CCS network problems. This section is not intended to provide the user with the solutions to CCS network problems, but to give a broad brush approach to determine the types of problems and isolation of the problems to the switch CNI ring, signaling link components and facilities, or the STP.

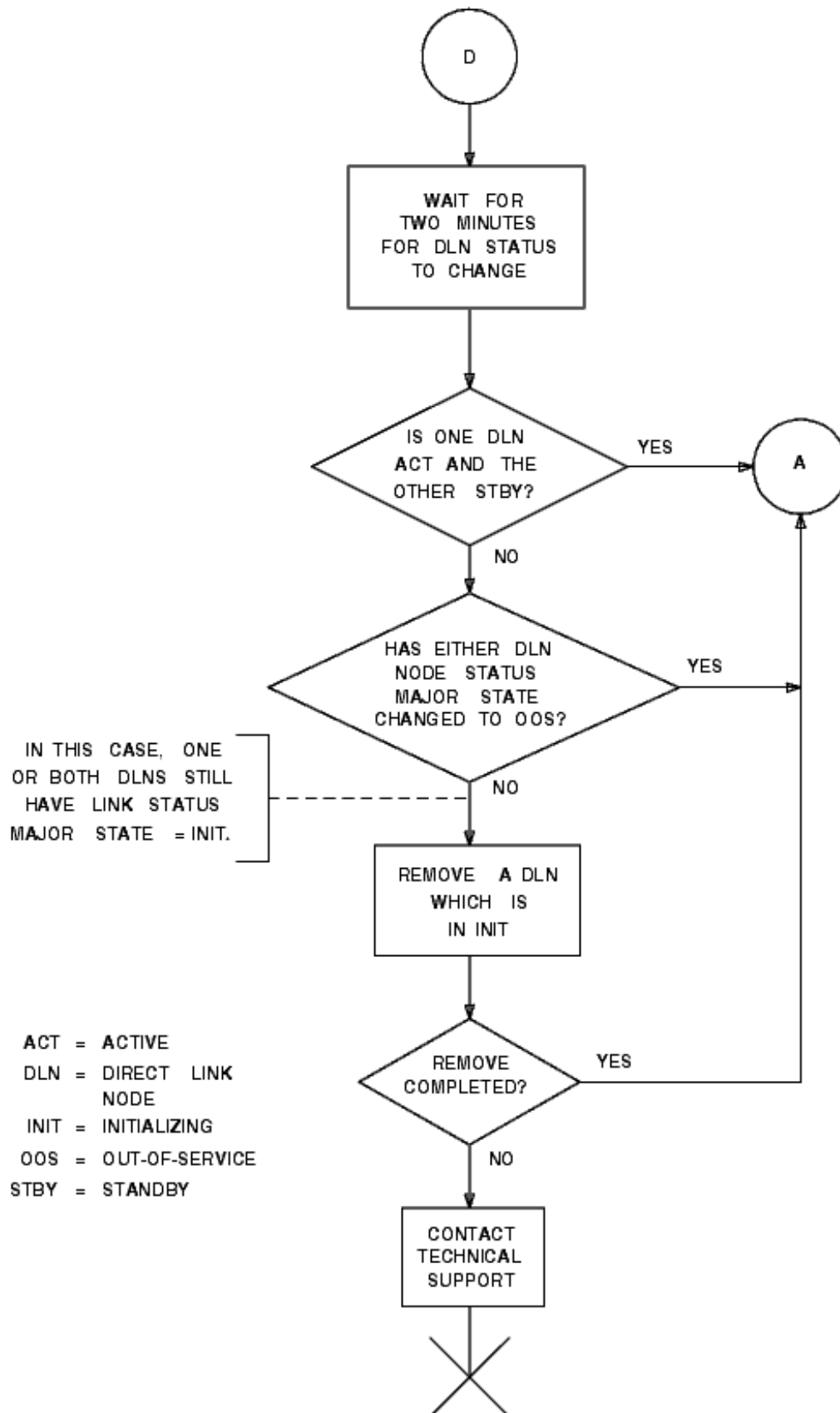
8.7.2 Problem Analysis Flow Diagrams

Figure 8.7-1 shows how to identify the problem indicators in the 112 Page, 118 Page, and the read-only printer messages. Tables 8.7-1, 8.7-2, and 8.7-3 give the description of the status indicators on the 118 Page. Figure 8.7-1 (Sheet 2) depicts a diagram for trouble isolation when the loss of service is due to DSIG, TCAP, or TSIG initialization. Figure 8.7-1 (Sheet 3) shows a diagram for determining if loss of service is caused by link node (RPCN, DLN, or LN) out of service. Figure 8.7-1 (Sheet 4) shows a diagram for determining that loss of service is due to signaling link out of service. Figure 8.7-1 (Sheet 5) shows a diagram for determining that loss of service is due to network problems.









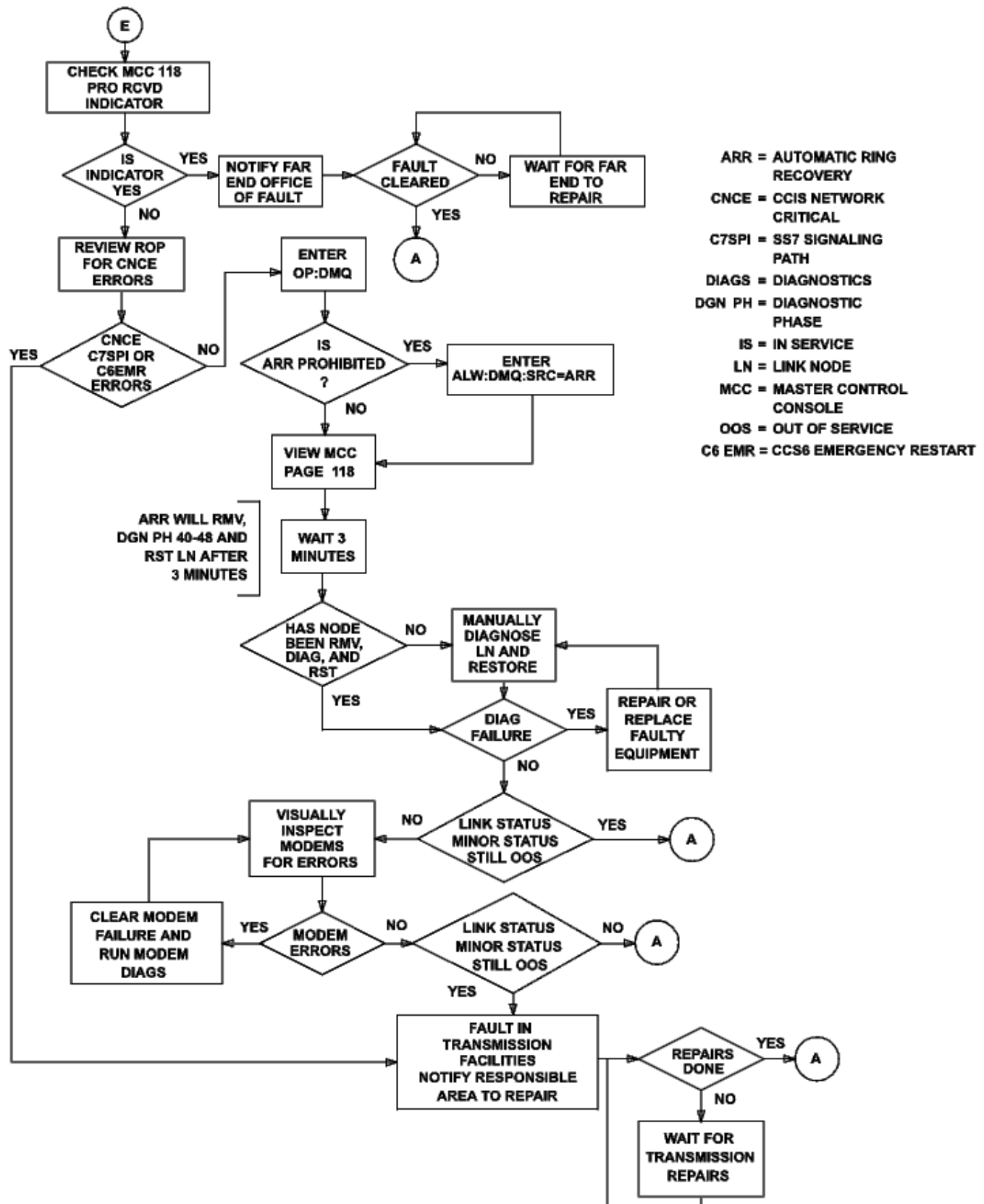


Figure 8.7-1 CNI Problem Indicators

Table 8.7-1 118 Page Status Indicators

FUNCTION OR COMPONENT	STATUS INDICATOR	DESCRIPTION
DSIG	UNEQUIP	Direct signaling is not equipped if: GLDSSPEED = 48 and no ECIS links are equipped GLDSSPEED = 560 and no SS7 links are equipped
	OOS	Direct signaling is out of service if DLN is equipped but: - Active DLN is not available. - Either DLN queue is in the growth state. GLDSSPEED = 48 and ECIS links are equipped but: - No ECIS links active. - Any active ECIS link is congested. - Any active ECIS link's far-end STP is congested (network problem). GLDSSPEED = 560 and SS7 links are equipped but: - Any SS7 link has a congestion level > 1. - Both STPs' point codes are not accessible (could be that no SS7 link is active). - Either STP has congestion level > 1 (network problem).
	ACT	The direct signaling service is active if: GLDSSPEED = 48 and ECIS links equipped, and: - At least one ECIS link is active. - No active ECIS link is congested. - No active ECIS link's STP is congested. GLDSSPEED = 560 and SS7 links equipped, and: - No SS7 link has a congestion level > 1. - At least one of the local STP's point codes are accessible. - Neither STP has a congestion level > 1. DLN is equipped and: - Active DLN is available. - Neither DLN queue is in the growth state.
	DGR	DSIG service is degraded. Indicates that either signaling link or DLN

TSIG		congestion exists.
	UNEQUIP	The trunk signaling service is not equipped if the data base relation <code>PCL_PRT</code> is not populated.
	OOS	The trunk signaling service is out of service when: • No ECIS or SS7 link is active, or is active and congested (near- or far-end). • DLN is equipped but: — Active DLN is not available. — Either DLN queue is in the growth state.
	ACT	The trunk signaling service is active when all of the following are true: • At least one ECIS or SS7 link is active, or active and congested (near- or far-end). • DLN is equipped and: — Active DLN is available. — Neither DLN queue is in the growth state.
	DGR	TSIG service is degraded. Indicates that either signaling link or DLN congestion exists.
TCAP	UNEQUIP	TCAP service is not equipped if: • Data base relation <code>DS_APP</code> is not populated. • No SS7 links exist.
	OOS	TCAP signaling service is down if: • Any SS7 link has congestion level > 1. • Neither of the point codes requiring global title translation are accessible. These point codes may be local STPs, remote STP pair, or one alias point code. This can be when no SS7 link is active. • The congestion level for either point code requiring global title translation is > 1 (network problem). • The DLN is equipped but: — Active DLN is not available. — Either DLN queue is in growth state.
	ACT	The TCAP signaling service is active when all of the following are true: • No SS7 link has congestion > 1. • At least one point code requiring global title translations is accessible.

		- The congestion level of both point codes requiring global title translation is not greater than 1. - The DLN is equipped and: - Active DLN is available. - Neither DLN queue is in the growth state.
	DGR	TCAP service is degraded. One or more of the following conditions exist: - Signaling link congestion exists. - DLN congestion exists. - A local subsystem failed (one or more but not all). - Global Title failed for a subsystem (one or more but not all).

Table 8.7-2 118 Page Status Indicators — Node State

NODE STATE	STATUS INDICATOR	DESCRIPTION
MAJOR	UNEQ	Node is unequipped but equipment configuration data exists.
	GROW	The node is physically being added or removed from the ring.
	OOS	The node is out of service and unavailable for service except for maintenance and diagnostics.
	OFL	The node is OOS and neither restoral nor removal is permitted.
	STBY	The node is an RPCN that is operating, but the ring configuration is not complete. The ring is down.)
	ACT	The node is active and performing on-line functions.
MINOR	NORM	Node is included in the active ring and is not a BISO or EISO node.
	BISO	This node is included in the active ring and forms the beginning of an isolated segment.
	EISO	This node is included in the active ring and forms the end of an isolated segment.
	ISO	This node is contained in the isolated segment.

Table 8.7-3 118 Page Status Indicators — Signaling Link

SIGNALING LINK STATE		DESCRIPTION
MAJOR	MINOR	
AVL	IS	Link available and in service operating normally.
AVL	OOS	Link taken out of service by CNI process.
AVL	MOOS	Link was manually removed with CHG:SLK message at either the near-end or far-end of link.
UNAV	GROW	Link is being added to system and is available for diagnostics.
UNAV	TEST	Link is unavailable for normal use. This state is used for sending test messages only. This is same as GROW, except ACTIVE/OOS timers are administered.
UNEQ	NONE	No signaling link exists.
INIT		This will show as a signaling link major state when the DLN is being pumped with office dependent data and CNI data.
STDBY		This will show as a signaling link major state when the DLN is in the standby state.
OOS		This will show as a signaling link major state when the DLN is out of service.

9. ISDN USER-NETWORK INTERFACE AND ISUP INTERWORKING

9.1 DESCRIPTION

The Q.931/ISDN User Part (ISUP) Interworking provides the logical mapping of signaling information between the Q.931 Integrated Services Digital Network (ISDN) access protocol and the SS7 ISUP network protocol for the establishment and clearing of basic circuit-switched (intra-LATA, inter-LATA, and international) calls. This includes the mapping of the messages, information elements/parameters, and corresponding fields between these two protocols. The Q.931/ISUP interworking also provides interworking capabilities necessary to support a number of call associated supplementary features and services which are accessible via either basic rate interface (BRI) or primary rate interface (PRI).

For more detailed information on BRI/PRI, refer to 235-190-104, *ISDN Feature Descriptions*.

9.1.1 AVAILABILITY

The Q.931/ISUP interworking capabilities were available with the 5E7 software release. Prior to the 5E6 release, ISUP trunks could be used to make calls between switches, but ISDN functionality (for example, backward call indicator mapping, PROGRESS, or ALERTING to caller showing exact status of the called party, etc.) was lost at the signal interface points (SIP). A SIP is defined as a point where the Q.931 signaling information is mapped to/from the ISUP protocol or vice versa.

Functionality was enhanced in the 5E7 software release to provide a more complete mapping between the Q.931 and ISUP protocols.

9.1.2 Q.931 BACKGROUND

9.1.2.1 ISDN User-Network Interface

The ISDN user-network interface protocol recommended by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-TS)(formerly CCITT) is often referred to as Q.931 protocol. This recommended protocol covers the procedure for establishing, maintaining, and clearing network connections at the ISDN user-network interface. The protocol procedure is defined in terms of messages exchanged over the D-channel of a BRI or PRI.

9.1.2.2 Message Definitions

The ISDN circuit-switched calls are controlled by a sequence of messages flowing across the user-network interface. The following Q.931 protocol messages are discussed in relationship to the phase of the call in which they are used.

- **Call Establishment Messages:**

ALERTING: (ALERT) The alerting message is returned to the calling user from the called user through the network to indicate that alerting has been initiated at the called user's terminal.

PROGRESS: (PROG) To indicate events associated with the call; for example, the applying of tones and announcements.

CALL PROCEEDING: (CALL PROC) This message acknowledges that call establishment has been initiated, and no more establishment information is accepted.

CONNECT: (CONN) This message returned by the called user to the calling user indicates call acceptance.

CONNECT ACKNOWLEDGE: (CONN ACK) Acknowledges receipt of a connect message.

SETUP: (SETUP) This message is sent by the user or the network to indicate call establishment.

SETUP ACKNOWLEDGE: (SETUP ACK) Acknowledges receipt of a setup message.

DISCONNECT: (DISC) This message is sent by the user or the network requesting the channel and call reference to be released.

RELEASE: (REL) This message is sent by either the user or the network to indicate that the equipment sending the message has disconnected the channel and intends to release the call reference. Therefore, the receiving equipment releases the channel and call reference.

RELEASE COMPLETE: (REL COMP) This message is sent by either the user or the network to indicate that the equipment sending the message and the receiving equipment has released the channel and call reference and the channel is available for reuse.

- **Other Messages:**

INFORMATION: (INFO) This message is sent by the BRI user to the network or by the network to the BRI user to provide additional information for call establishment, identify channel negotiation, and request or provide status on facilities.

RESTART: (REST) This message is sent from one end of the connection to the other to request a return to the idle condition on the indicated channel.

RESTART ACK: (REST ACK) This message is returned from the recipient of the RESTART message to acknowledge compliance with the restart request.

SERVICE: (SERV) This message is used to update the service status of a channel (applies to PRI only).

SERVICE: (SERV ACK) Acknowledges receipt of a service message (applies to PRI only).

STATUS: (STAT) This message may be sent by either the user or the network at any time during a call when an unexpected message is received or to report other conditions of the call.

STATUS ENQUIRY: (STAT ENQ) This is a message sent by either the user or the network requesting a status message.

Each message is comprised of individual information elements. These elements provide information to various equipment components that are involved in the message processing (for example, length of message, connected address, calling party number, cause values, etc.).

9.1.2.3 Message Processing

See 235-900-32x, *ISDN Basic Rate Interface Specification*, and 235-900-33x, *ISDN Primary Rate Interface Specification*, for more information on protocol errors.

NOTE: The x in these document numbers corresponds to the specific software release of the document.

9.2 IMPLEMENTATION

9.2.1 Network Configuration

Figure 9.2-1 illustrates the call processing for a simple circuit-switched call. The 5ESS®-2000 switches shown are the signaling interface points (SIP).

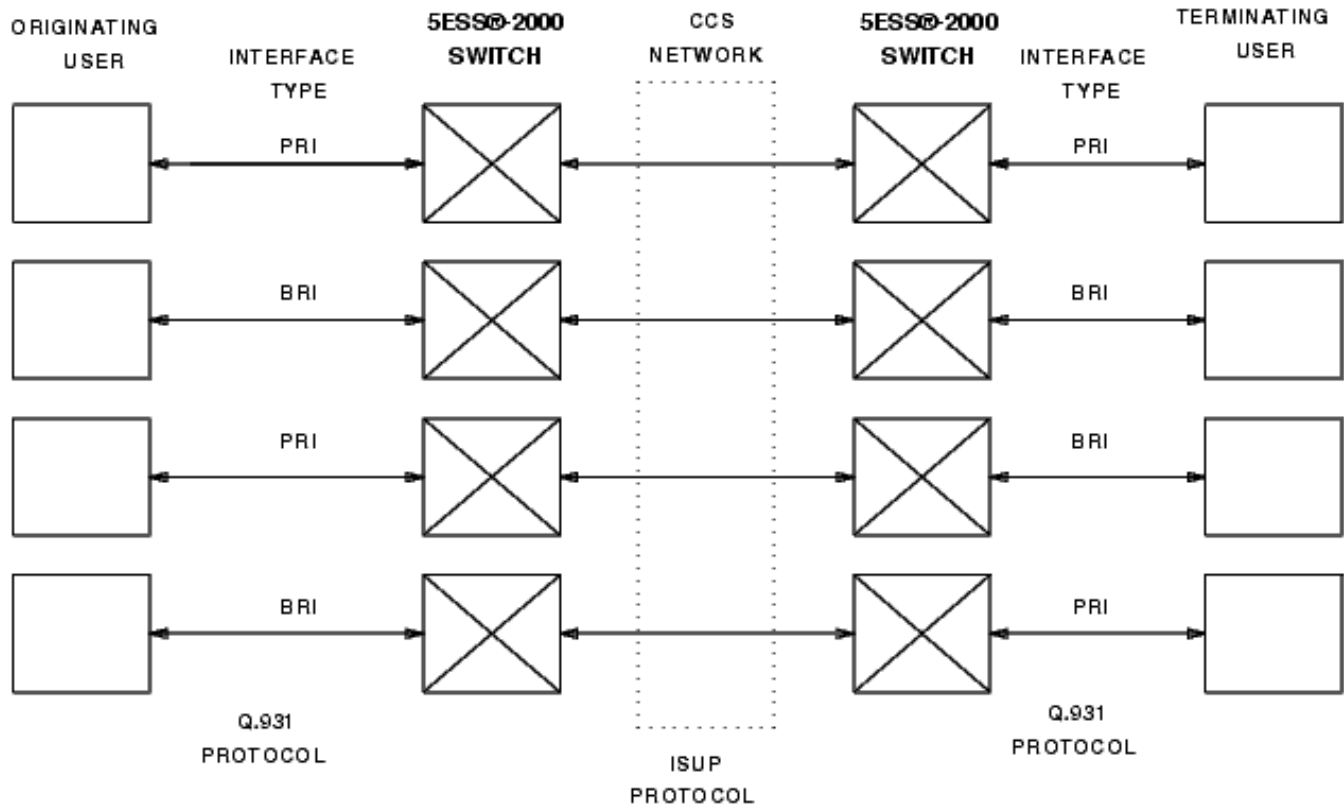


Figure 9.2-1 Processing of a Q.931/ISUP Call Through the 5ESS -2000 Switch

9.2.2 ISDN User Part (ISUP) Description

The term ISUP refers to the Signaling System 7 (SS7) protocol for ISDN signaling over the CCS network. See "ISDN USER PART (ISUP)," Section 5 for details concerning the ISUP feature.

9.2.3 Q.931/ISUP Interworking Feature Description

This feature allows the switch to support the ISDN interswitch operation by providing signaling mapping for end-to-end ISDN circuit-switched voice and data connections using the SS7 network. When the Q.931 protocol signaling is received by the switch, the mapping translates the signaling information into outgoing ISUP messages destined for the distant ISDN user. At the distant end, the ISUP messages are translated back into the Q.931 protocol format and delivered to the distant ISDN user. Response messages from the distant ISDN user are handled by mapping in the same way.

Access to the switch by the ISDN customer is either through a PRI or through a BRI [also known as a digital subscriber line (DSL)]. These interfaces may be 56 kb/s, 64 kb/s restricted, or 64 kb/s clear channels.

9.2.4 Message Mapping From ISDN To ISUP Protocols

A subset of Q.931 signaling messages used by BRI and PRI for basic call setup and call clearing procedures are mapped into the ISUP protocol.

Table 9.2-1 lists the signaling messages used in Q.931 that are mapped to ISUP messages for interswitch calls.

Table 9.2-1 Message Mapping From ISDN User Protocol To ISUP Protocol

ISDN USER MESSAGE	SIGNALING DIRECTION ^a	ISUP MESSAGE	CONDITION
SETUP	→	IAM	
INFORMATION	→	IAM	BRI Overlap Sending
ALERTING ^b	←	ACM	
PROGRESS	←	CPG ^c	
PROGRESS	←	ACM	
ALERTING ^b	←	CPG ^c	
CONNECT	←	ANM	
DISCONNECT	←→	REL	
RELEASE	→	REL	First Clearing Message
RELEASE COMPLETE	→	REL	First Clearing Message

Notes:

a. Following are the definitions of the directional arrows:

→ Q.931 message traveling from originating user

← Q.931 message traveling to originating user

←→ Q.931 message sent in either direction

b. Only one ALERTING message is sent.

c. Early CPG received prior to ACM is mapped.

9.2.5 Message Mapping From ISUP To ISDN Protocols

Table 9.2-2 contains the significant ISUP signaling messages that concern the interworking capability. The ISUP messages listed in Table 9.2-2 are mapped over to Q.931 protocol messages.

Table 9.2-2 Message Mapping from ISUP Protocol To ISDN User Protocol

ISUP MESSAGE	SIGNALING DIRECTION ^a	ISDN USER MESSAGE	CONDITION
IAM	→	SETUP	
ACM	←	ALERTING	
CPG	←	PROGRESS	When ACM Was Previously Sent.
ACM	←	PROGRESS	
CPG	←	ALERTING	When ACM Was Previously Sent.
ACM	←	CONNECT ^b	If First Response To SETUP.
ANM	←	CONNECT ^b	
FRJ (Facility Reject)	←	STATUS (Cause=43) ^c	Not Supported in Local Networks.
REL	←→	DISCONNECT	
REL COMPLETE	←	REL	First Clearing Message.

Notes:

a. Following are signaling direction symbol definitions:

→ Q.931 message to a terminating user

← Q.931 message from a terminating user

↔ Q.931 message sent in either direction

Although a CPG can be sent in the forward direction, it is not mapped to a Q.931 message. A CPG message received in the talking state is not mapped to a Q.931 message.

- b. Fast connect sends only ANM.
- c. A cause of 43 indicates that the user information was discarded because the total length of MA-UUI information elements exceed 64 bytes.

9.2.6 Information Elements And Parameters

The ISUP messages are comprised of parameters and are described in TR-NWT-000246 (Q.763) Bellcore Specification of Signaling System Number 7. The Q.931 messages are comprised of information elements (IE) and are described in 235-900-34x, *ISDN Basic Rate Interface Specification*, and 235-900-34x, *ISDN Primary Rate Interface Specification*.

NOTE: The x in these document numbers corresponds to the specific software release of the document.

At a signaling interface point, when interworking occurs, ISUP parameters are mapped to Q.931 IEs or vice versa. Not all ISUP parameters are mapped to corresponding IEs, and not all IEs are mapped to ISUP parameters. Additionally, some parameters or IEs may be generated at the SIP independent of the interworking function.

Tables 9.2-3 , 9.2-4 , 9.2-5 , 9.2-6 , 9.2-7 , 9.2-8 , 9.2-9 , 9.2-10 , 9.2-11 , and 9.2-12 detail the mapping of Q.931 messages and IEs to ISUP messages and parameters (and the reverse) which takes place at a switch signaling interface point.

Table 9.2-3 Mapping of Q.931 REL, REL COMP, or DISC to an ISUP ACM, CPG, or REL

REL/REL COM/DISC	DIRECTION	ACM/CPG/REL	MAPPING NOTES
Cause	→	Cause	Mapped to Cause Parameter. Mapped to Cause and ATP for ACM.
Signal	(discarded)		
UUI	→	UUI	PRI Only
LS7	→	ATP	PRI Only

Table 9.2-4 Mapping of ISUP REL to Q.931 REL, REL COMP, or DISC

REL	DIRECTION	REL/REL COM/DISC	MAPPING NOTES
Cause	→	Cause	Mapped from ATP if present; otherwise, mapped from Cause Parameter
		Signal	Generated based on Cause
UUI	→	UUI	PRI Only
ATP	→ →	LS7 Cause	PRI Only Cause Mapped from ATP if present; otherwise, mapped from Cause Parameter

Table 9.2-5 Mapping of Q.931 CONNECT to ISUP ANM

CONNECT	DIRECTION	ANM	MAPPING NOTES
Signal	(discarded)		
Progress	(discarded)		
CN	→	ATP	PRI Only
RN	→	ATP	PRI Only

LS7	→	ATP	PRI Only

Table 9.2-6 Mapping of ISUP ANM to Q.931 CONNECT

ANM	DIRECTION	CONNECT	MAPPING NOTES
		Signal	Generated based on BCAP, BRI Only
		Progress	Generated based on BCI, BRI Only
ATP	→	CN	PRI Only
	→	RN	PRI Only
	→	LS7	PRI Only

Table 9.2-7 Mapping of Q.931 ALERTing to ISUP ACM or CPG

ALERTING	DIRECTION	ACM/CPG	MAPPING NOTES
		Event Information	Generated by Switch
RN	→	ATP	PRI Only
LS7	→	ATP	PRI Only
UUI	→	UUI	PRI Only

Table 9.2-8 Mapping of ISUP ACM or CPG to Q.931 ALERTING

ACM/CPG	DIRECTION	ALERTING	MAPPING NOTES
		Signal	Generated based on Event Ind. BRI Only
		Progress	Generated based on BCI, BRI Only
ATP	→	RN	PRI Only
	→	LS7	PRI Only
UUI	→	UUI	PRI Only

Table 9.2-9 Mapping of Q.931 PROGRESS to ISUP ACM or CPG

PROGRESS	DIRECTION	ACM/CPG	MAPPING NOTES
Cause	→	Cause	Mapped to Cause and ATP Parameters
		Event Information	Generated by Switch
Progress	(discarded)		
RN	→	ATP	PRI Only
LS7	→	ATP	PRI Only
UUI	→	UUI	PRI Only

Table 9.2-10 Mapping of ISUP ACM or CPG to Q.931 PROGRESS

ACM/CPG	DIRECTION	PROGRESS	MAPPING NOTES
Cause	→	Cause	Mapped from Cause Parameter. If none present, mapped from ATP
		Signal	Generated based on Event Ind. BRI Only
		Progress	Generated based on BCI, BRI only
ATP	(discarded)		
UUI	(discarded)		

Table 9.2-11 Mapping of Q.931 SETUP to ISUP IAM

SETUP	DIRECTION	IAM	MAPPING NOTES
BCAP	→	USI	
CPN	→	CPN	Mapped for User Provided Passed Screening CPNs Only
KP	→	CdPN	BRI Only
		TNS	BRI Only
CdPN	→	CdPN	For PRI. Added for N-ISDN1 BRI if Functional Addressing used.
OSA	→	CdPN	Added for N-ISDN BRI if Functional Addressing used
TNS	→	TNS	For PRI.

			Added for N-ISDN1 BRI if Functional Addressing used.
Signal	(discarded)		
UUI	→	UUI	PRI Only
LLC	→	ATP	N-ISDN1 BRI Only
HLC	→	ATP	N-ISDN1 BRI Only
CgPS	→	ATP	N-ISDN1 BRI Only
CdPS	→	ATP	N-ISDN1 BRI Only
RN	→	ATP	PRI Only
LS7	→	ATP	PRI Only
LS6	(discarded)		

Table 9.2-12 Mapping of ISUP IAM to Q.931 SETUP

IAM	DIRECTION	SETUP	MAPPING NOTES
USI	→	BCAP	
CPN	→	CPN	
GAP	(discarded)		
CdPN	→	CdPN	For PRI Only. Added for N-ISDN1 BRI.
OCN	→	RN (1st)	N-ISDN BRI only
RN	→	RN (1st)	N-ISDN BRI only
RI	→	RN (1st and 2nd)	N-ISDN BRI only
TNS	→	TNS	PRI Only
UUI	→	UUI	PRI Only
ATP	→	PROGress	BRI and PRI
ATP	→	LLC	
ATP	→	HLC	N-ISDN1 BRI Only
ATP	→	CgPS	N-ISDN1 BRI Only
ATP	→	CdPS	N-ISDN1 BRI Only
ATP	→	RN	PRI Only
ATP	→	LS7	PRI Only

9.2.7 Routing Considerations

The call message and routing data structure contains fields which are used by the switch trunk routing mechanism to enforce various routing restrictions for CCS calls. This is commonly known as the "traveling class mark" of a call. The trunk data can accommodate routing restrictions imposed by the "traveling class mark." This same mechanism is used to accommodate routing restrictions from calls that interwork between the ISUP trunks and ISDN BRI/PRI lines/trunks. An example of a common routing restriction is to limit a call from going through another satellite link when one satellite link has already been used in the end-to-end call path.

For ISUP originated calls, values in the routing data structure are populated to assure that call routing is ISUP preferred. This means that routing attempts to select another ISUP trunk, but does not kill the call if no ISUP trunks are available, the call is routed to a non-ISUP trunk. To administer ISUP preferred routing, ISUP trunks, PRI trunks, or a BRI termination must be populated in the routing domain of all ISUP/PRI trunks or BRI lines.

For data calls, bearer capability sensitive routing is used to route data calls to trunks which support the data speed of a particular call.

9.2.8 Sequence Of Events For Successful Call Setup

The following explains the message flow events for messages involved in a call placed from an ISDN user through the SS7 network to another ISDN user.

- **From originating user to originating switch**

SETUP: When the user initiates a call, a SETUP message is sent by the BRI/PRI terminal to the switch.

- ***From originating switch to originating user***

CALL PROCEEDING: If the information is complete, a CALL PROCEEDING message is sent to the originating terminal.

- ***Interswitch call setup***

INITIAL ADDRESS MESSAGE (IAM):

- The originating switch maps the information into an outgoing ISUP IAM.
- The IAM message is transmitted to the terminating switch via the CCS network.
- After the IAM message has been sent, the originating switch waits for the response from the terminating switch.

ADDRESS COMPLETE MESSAGE (ACM): When either an ALERTING or PROGRESS message is received from the BRI/PRI terminal, the terminating switch transmits the ACM back to the originating switch via the CCS network.

CONNECT MESSAGE: When the terminating party goes off-hook, a CONNECT message is sent to the originating user.

- The terminating switch maps the CONNECT message into an outgoing ISUP ANSWER (ANS) message.
- The ANSWER message is transmitted back to the originating switch indicating that the call has been answered.
- The originating switch maps the information from the ANSWER message back into the CONNECT message for delivery to the originating terminal.

DISCONNECT MESSAGE: When either the terminating or originating party goes on-hook, a DISCONNECT message is sent from the disconnecting party to the switch.

RELEASE MESSAGE:

- When one of the processes hangs up, the switch maps the DISCONNECT message into an outgoing ISUP RELEASE (REL) message.
- The RELEASE message is transmitted indicating that the circuit identified in the message is being released due to the reason supplied and is ready to be put in the idle state.
- On receipt of the RELEASE message, the switch maps the information from the RELEASE message back into the DISCONNECT message and sends it to the originating/terminating terminal.

RELEASE COMPLETE MESSAGE: This message is sent to indicate that the circuit concerned has been brought into the idle condition and is only sent from one switch to another but never passed through a switch.

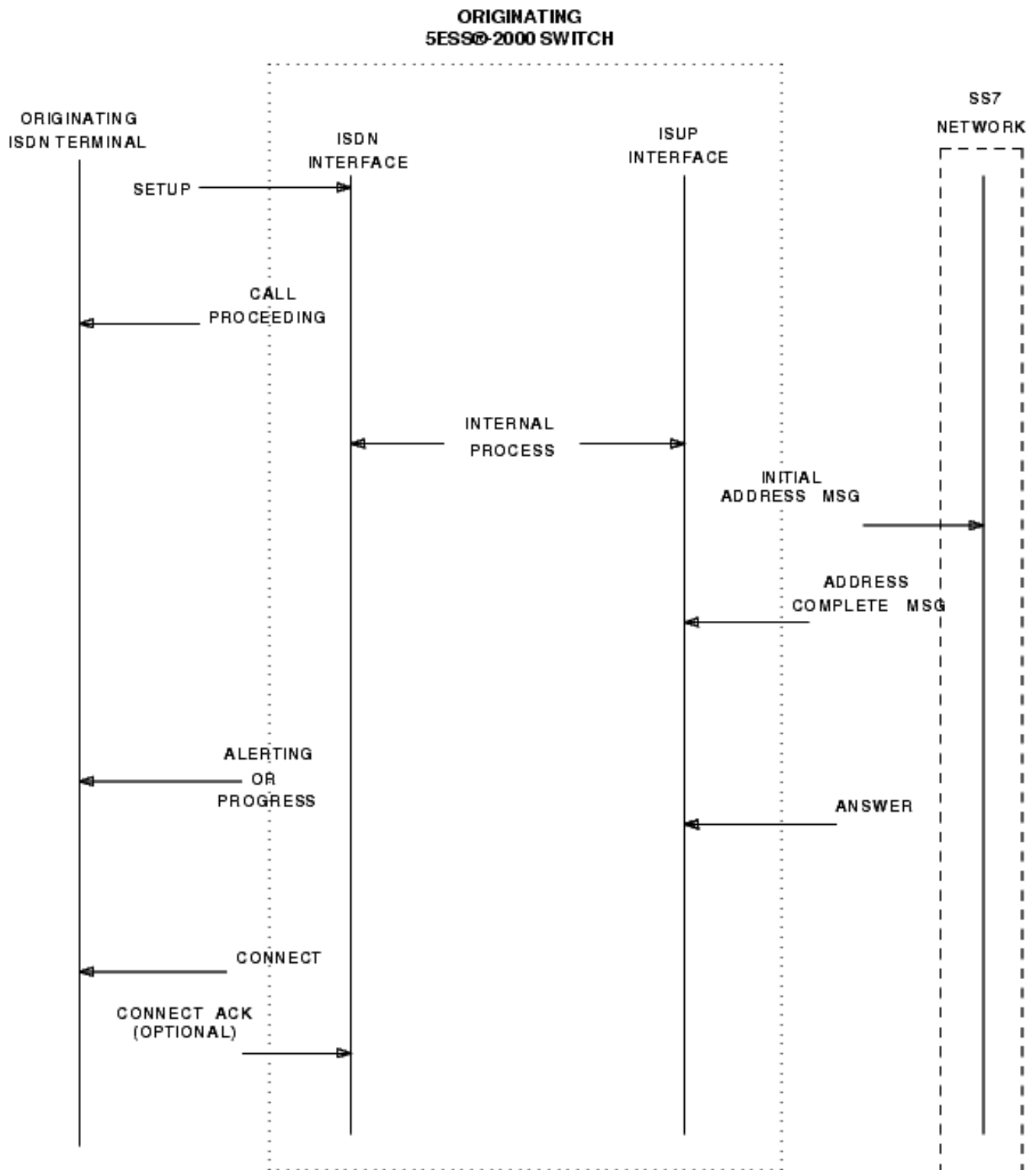
9.2.8.1 Message Flow

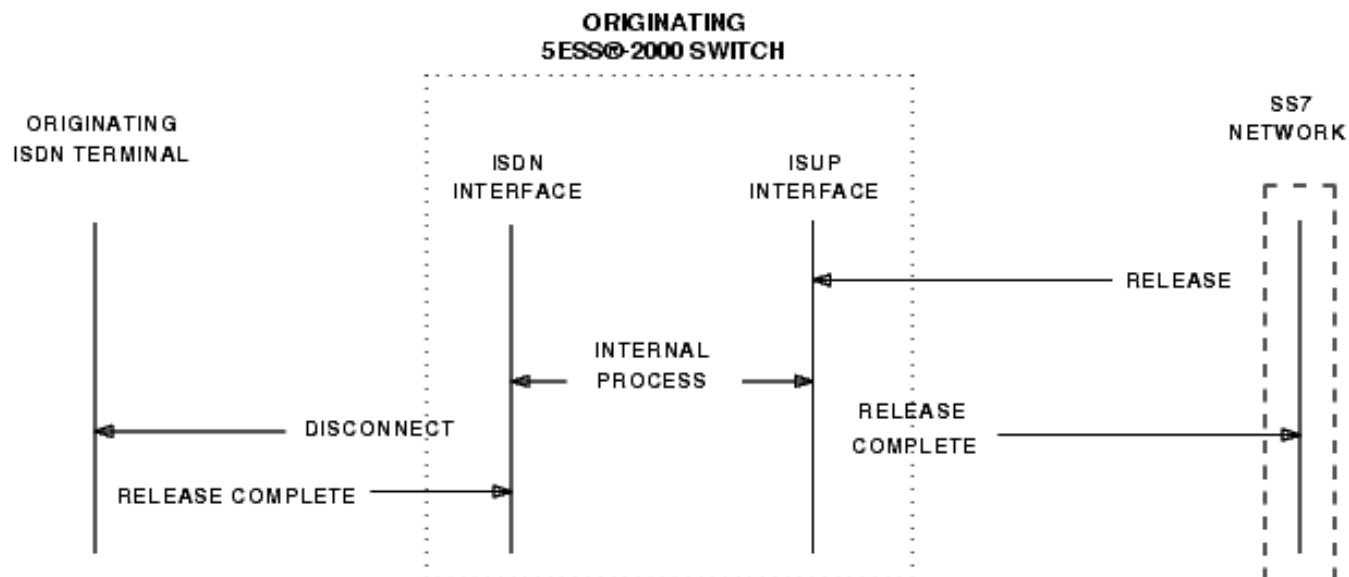
Figure 9.2-2 illustrates the call setup message flow from the originating user through the switch to the CCS network.

Figure 9.2-3 illustrates the message flow at the terminating switch from the CCS network to the terminating user.

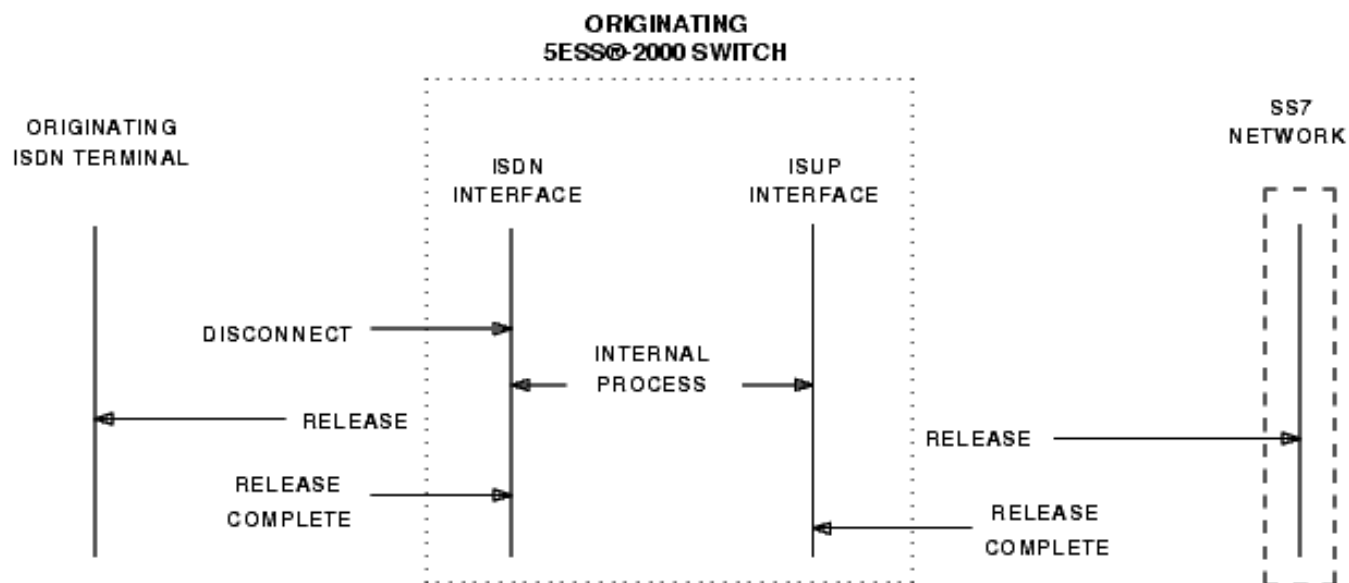
Figure 9.2-4 illustrates the message flow when a call fails. Figure 9.2-5 illustrates the message flow for generating

announcements when a call fails.





A. CALLED PARTY DISCONNECTS FIRST



B. CALLING PARTY DISCONNECTS FIRST

Figure 9.2-2 ISDN/ISUP Message Flow Originating End

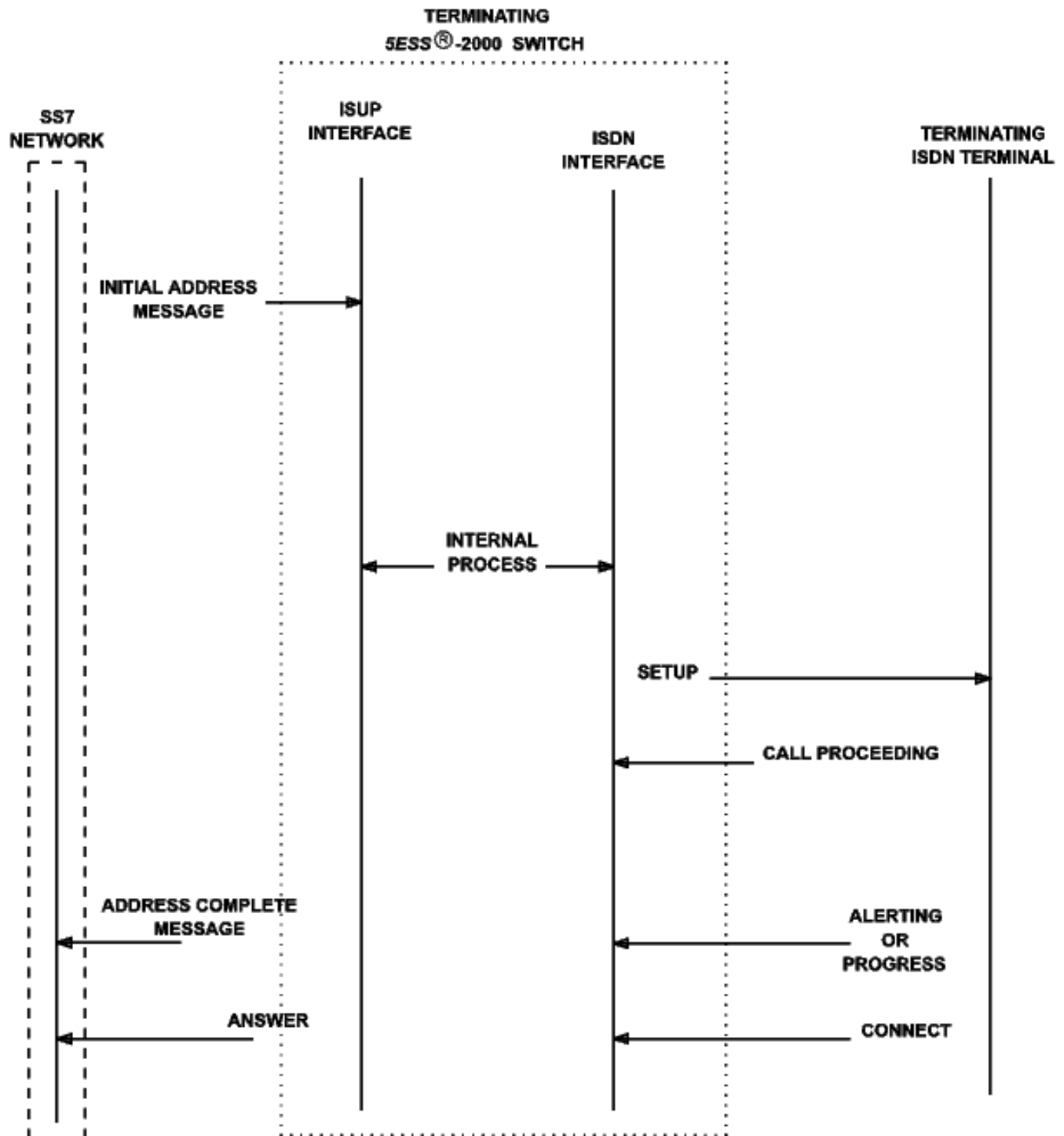


Figure 9.2-3 ISDN/ISUP Message Flow Terminating End

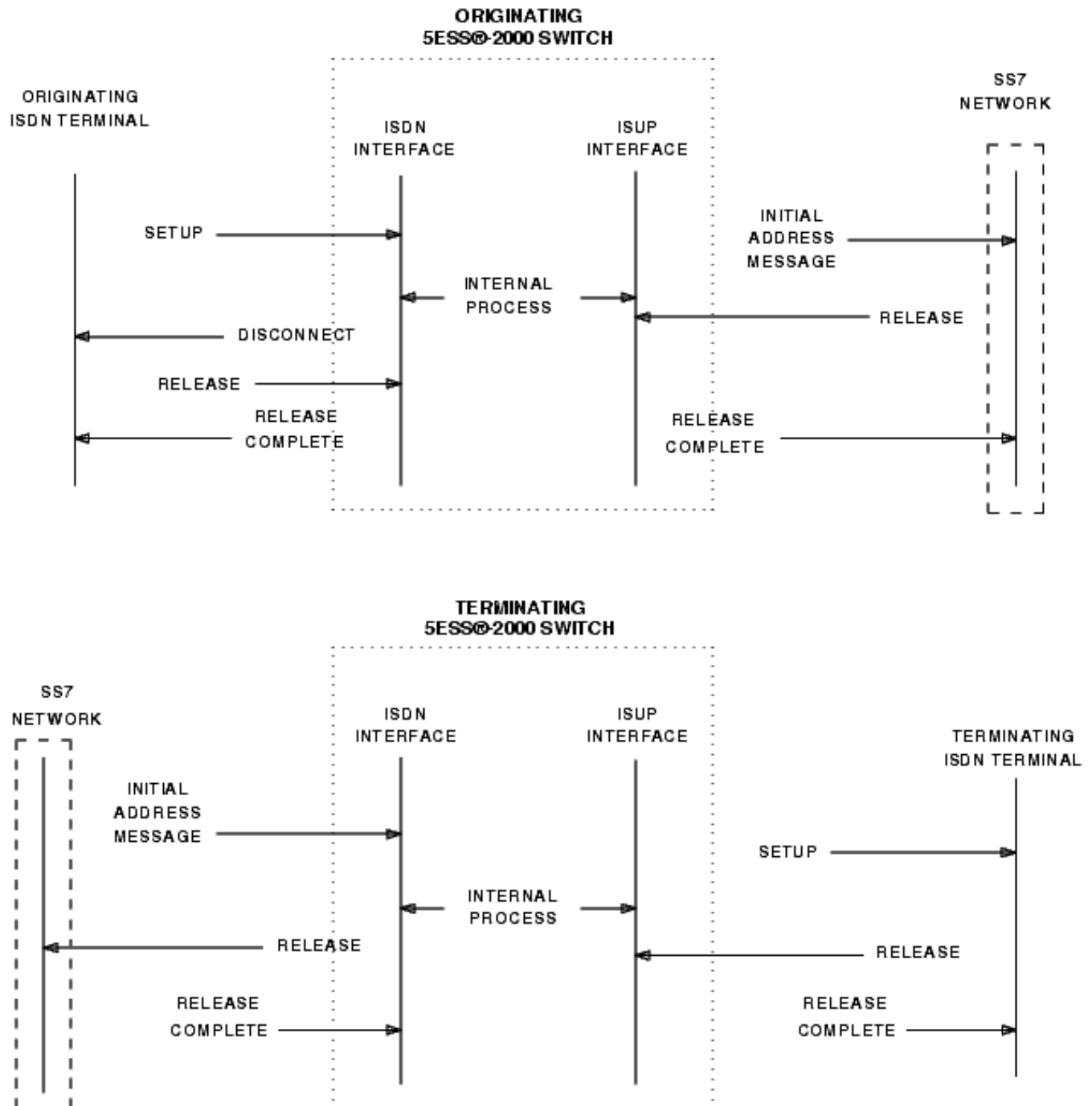


Figure 9.2-4 Call Failure Message Flow ISDN/ISUP

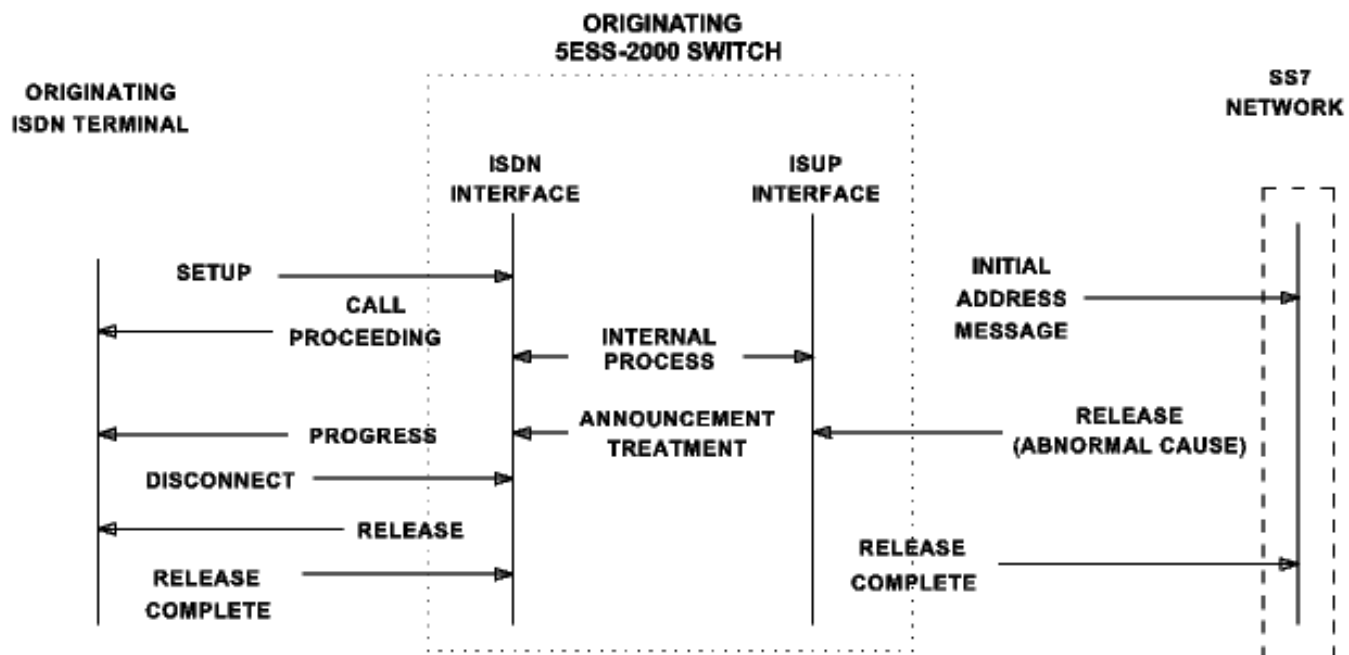


Figure 9.2-5 Call Failure Message Flow ISDN/ISUP Announcements

9.3 USER-TO-USER INFORMATION TRANSPORT

The ISDN Q.931 to ISUP Interworking feature includes the mapping of Q.931 Message Associated User-to-User Information (MA-UUI) Elements between the ISUP and the Q.931 protocols. This feature allows BRI/PRI users to send user-defined data as part of signaling information during setup and clearing of circuit-switched calls. This information is not interpreted by the network, but is transparent to the network and is delivered to the terminating end-user. The term MA-UUI does not just refer to the UUI information element that is part of the Q.931 message, but rather is more general and refers to all the user-defined data that can be placed in several information elements including the UUI. These information elements are summarized in Table 9.3-1. If the network is not all SS7, the user-defined MA-UUI is lost.

The MA-UUI elements may be included in the following Q.931 messages:

- SETUP
- ALERTING
- PROGRESS
- CONNECT
- DISCONNECT.

The ISUP Access Transport Parameter (ATP) and User-to-User (UUI) Parameter are capable of transporting 129 octets (not including the identifier octet and the length octet) of user information. However, the switch Q.931 implementation only allows 64 octets of data for the combined length of the *User-to-User Information Element* and the *User Data Information Elements*.

Table 9.3-1 MA-UUI Information Element Summary

MA-UUI IE	DESCRIPTION	USERS SUPPORTED ^a	ISUP PARAMETER
CN	Connected Number IE is used to indicate the address connected to a call. The CN may be different from the calling or called party due to forwarding or transferring a call.	PRI	ATP
RN	Redirecting Number IE is used to identify the Called Party Number from which Call Forwarding or Call Transfer occurred.	PRI	ATP
LLC	Low Layer Compatibility IE provides a user-to-user compatibility checking mechanism.	PRI/BRI	ATP
HLC	High Layer Compatibility IE provides a user-to-user compatibility checking mechanism. (for example, to insure identical data rates).	BRI	ATP
UUI	User-to-User IE is used to convey a wide range of information between two end-users.	PRI	UUI
CdSA	Called Party Subaddress IE contains a user supplied identifier, such as a password or terminal ID	BRI	ATP
CgPS	Calling Party Subaddress IE contains a user supplied identifier, such as a password or terminal ID	BRI	ATP
LS7	Locking Shift to Code Set 7 IE indicates that the remaining IEs in the message should be interpreted according to the element identifiers in Code Set 7.	PRI	ATP
USC7	User Specific Code Set 7 IEs contain user data formatted using Code Set 7.	PRI	ATP
PIE	Progress IE is used to indicate a call event, such as "not end-to-end ISDN."	PRI/BRI	ATP
Notes:			

a.	BRI means National ISDN BRI and BRI.

9.3.1 Originating End Office

- Forward Messages

The *User-to-User Information Element* can be present in the Q.931 SETUP and DISCONNECT messages.

The ATP can be present in the IAM or REL message. The originating switch examines the total length of all the Q.931 *User Data Information Elements* the ISDN customer provides that can go into the ATP in forward messages. If the total length exceeds 64 octets (including each information element's identifier octet and length octet), all the Q.931 MA-UUI *information elements* are dropped and not mapped to the ATP. Otherwise, each *information element's* identifier octet and length octet is included along with each *information element's* content in the ATP.

- Backward Messages

The ATP can be present in the ACM, ANM, CPG, or REL messages. The originating switch will unpack the ATP and examine each Q.931 User Data IE in the ATP. If a Q.931 IE other than one those listed in Table 9.3-1 is found, that IE is considered unrecognized and is discarded. All recognized IEs remain in the ATP to be mapped to appropriate Q.931 messages.

If the total length of the received MA-UUI IEs received by the originating switch in the UUI and ATP parameters exceeds 64 data octets, the UUI is discarded. If the total length of the remaining MA-UUI IEs in the ATP still exceeds 64 data octets, the ATP is discarded and the information is not interworked.

When a UUI or ATP parameter is discarded, no ISUP Facility Reject message (FRJ) is generated. If an originating switch receives an FRJ, it does not map the FRJ into any Q.931 message.

9.3.2 Terminating End Office

- Forward Messages

A UUI parameter can be present in the IAM or REL message.

An ATP parameter can be present in an IAM or REL message. The terminating switch unpacks the ATP, and examines each Q.931 *User Data Information Element* in the ATP. If a Q.931 *Information Element* other than one of those shown in Table 9.3-1 is found in the ATP, that *information element* is considered *unrecognized* and is discarded. All the recognized *information elements* remain in the ATP.

If the total length of the received MA-UUI IEs received by the terminating switch in the UUI and ATP parameters exceeds 64 data octets, the UUI is discarded. If the total length of the remaining MA-UUI IEs in the ATP still exceeds 64 data octets, the ATP is discarded and the information is not interworked.

- Backward Messages

The *User-to-User Information Element* can be present in Q.931 ALERTING, CONNECT, and DISCONNECT messages.

The total length of all MA-UUI IEs to be mapped to the ATP and UUI parameters cannot exceed 64 octets (including each IEs identifier octet and length octet); otherwise, all the IEs are discarded and the information is not interworked.

When the MA-UUI IEs are discarded, a Q.931 STATUS message is sent to the user with a cause value of "User

information discarded," 43. A received FRJ message is not mapped into any Q.931 message.

9.3.3 ATP/UII Transport with Fast Connect

The fast connect message sequence is discussed in "Fast Connect CCS Message Flow," Section 9.4.1. The UII IE and any IEs to be transported in the ATP parameter are sent in the ACM message; the ANM message does not contain either the ATP or UII parameters. ATP and UII parameters, if they apply, are sent in the ANM message; no ACM message is sent for fast connect.

9.3.4 Cause Information Transport

The cause indicators parameter, which is implemented in ACM, carries the cause information.

9.3.4.1 Originating End Office

Because the cause *information element* can be transported in the ATP from a pre-5E7 software release switch, the originating switch must handle a cause parameter in the ATP as follows:

- For REL message received at the originating switch:
 - If the REL contains an ATP with a cause *information element*, the cause *information element* in the ATP is passed to the corresponding Q.931 message. The cause indicators parameter in the REL, if any, is discarded. In pre-5E7 software releases, a cause indicators parameter is considered unreliable.
 - If the REL does not contain an ATP, or the ATP in the REL does not contain a cause *information element*, then the cause indicators parameter in the REL is mapped to the cause *information element* of the corresponding Q.931 message.
- For other SS7 messages received at the originating switch:
 - If an SS7 message received contains a cause indicators parameter, the cause indicators parameter is mapped to the cause *information element* of the corresponding Q.931 message. If the ATP also contains a cause *information element*, it is discarded.
 - If the SS7 message received does not contain a cause indicators parameter, but it contains an ATP and the ATP contains a cause *Information Element*, the cause *information element* in the ATP is passed to the corresponding Q.931 message.

9.3.4.2 Terminating End Office

- For an ACM sent from the terminating switch:
 - Since a pre-5E7 software release only looks at an ATP for cause information in an ACM, the cause information is placed in both the cause indicators parameter and the ATP of an ACM.
- For other SS7 messages sent from the terminating switch:
 - The cause information is always carried by the SS7 cause indicators parameter of any SS7 messages. No cause *information element* is transported in the access transport parameter.

9.3.5 Coding Of Progress IE At The Terminating Exchange

At the terminating exchange, if an IAM is received and the user service information requested is supported by the terminating interface, and if the called line is ISDN and idle, a Q.931 SETUP message will be sent.

In the 5E6 software release, a Progress Indicator IE will only be included in the SETUP message when received in the ATP parameter of the incoming IAM.

In 5E7 and later releases, ISUP is included in the following cases:

- A Progress Indicator IE is received in the ATP in the IAM. A Progress Indicator IE in ATP is unexpected. However, if received, the specified procedure should be followed.

The Progress Indicator IE sent to the called party in the SETUP message is coded as received.

- A Progress Indicator IE is not included in the ATP received in the IAM, and the Interworking bit in the received Forward Call Indicators parameter, is coded "interworking encountered."

The progress description in the Progress Indicator IE in the SETUP message is "call is not end-to-end ISDN," and the general location is coded "network beyond the interworking point."

- A Progress Indicator IE is not included in the ATP received in the IAM, the Interworking bit in the received Forward Call Indicators parameter is coded "no interworking encountered," and the ISDN User Part Indicator bit is coded "ISUP used all the way," and the ISDN Access Indicator bit of the received Forward Call Indicators parameter is coded "originating access non-ISDN."

The Progress Indicator IE sent in the SETUP message should contain a progress description value coded "calling equipment is non-ISDN." The location code is coded "public network serving the remote user."

- Otherwise, a Progress Indicator IE is not included in the SETUP message.

9.4 SUPPORTED FEATURES AND SERVICES

9.4.1 Fast Connect CCS Message Flow

The Fast Connect feature is discussed in "Fast Connect," Section 5.3.1 of this document. Figures 9.4-1 and 9.4-2 illustrate the call flow for Fast Connect feature calls from the originating user through the switch to the CCS network. Figures 9.4-3 and 9.4-4 illustrate the fast connect call flow from the CCS network through the switch at the terminating user.

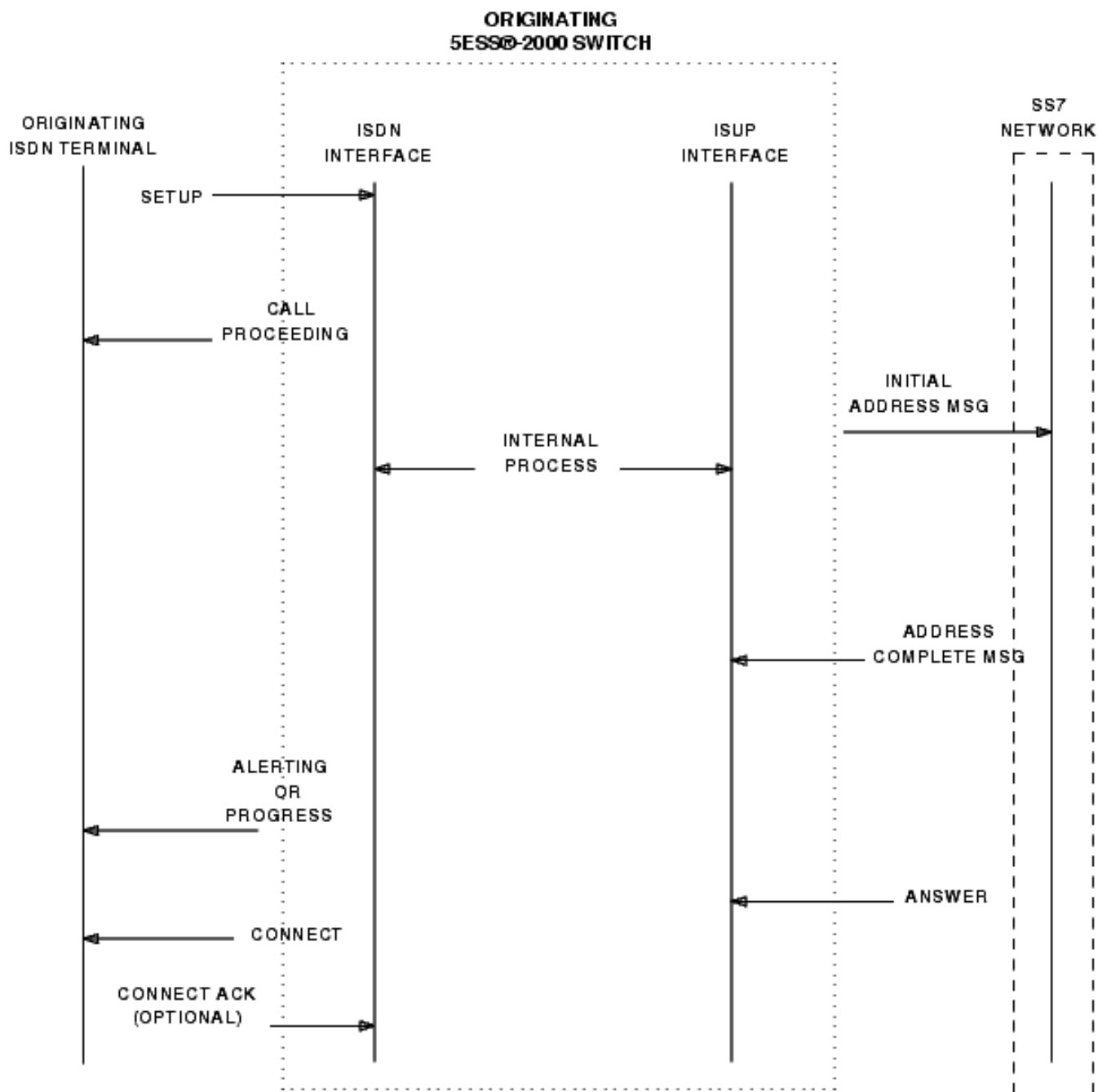


Figure 9.4-1 ISDN/ISUP Fast Connect Message Flow - Originating End - 5E6

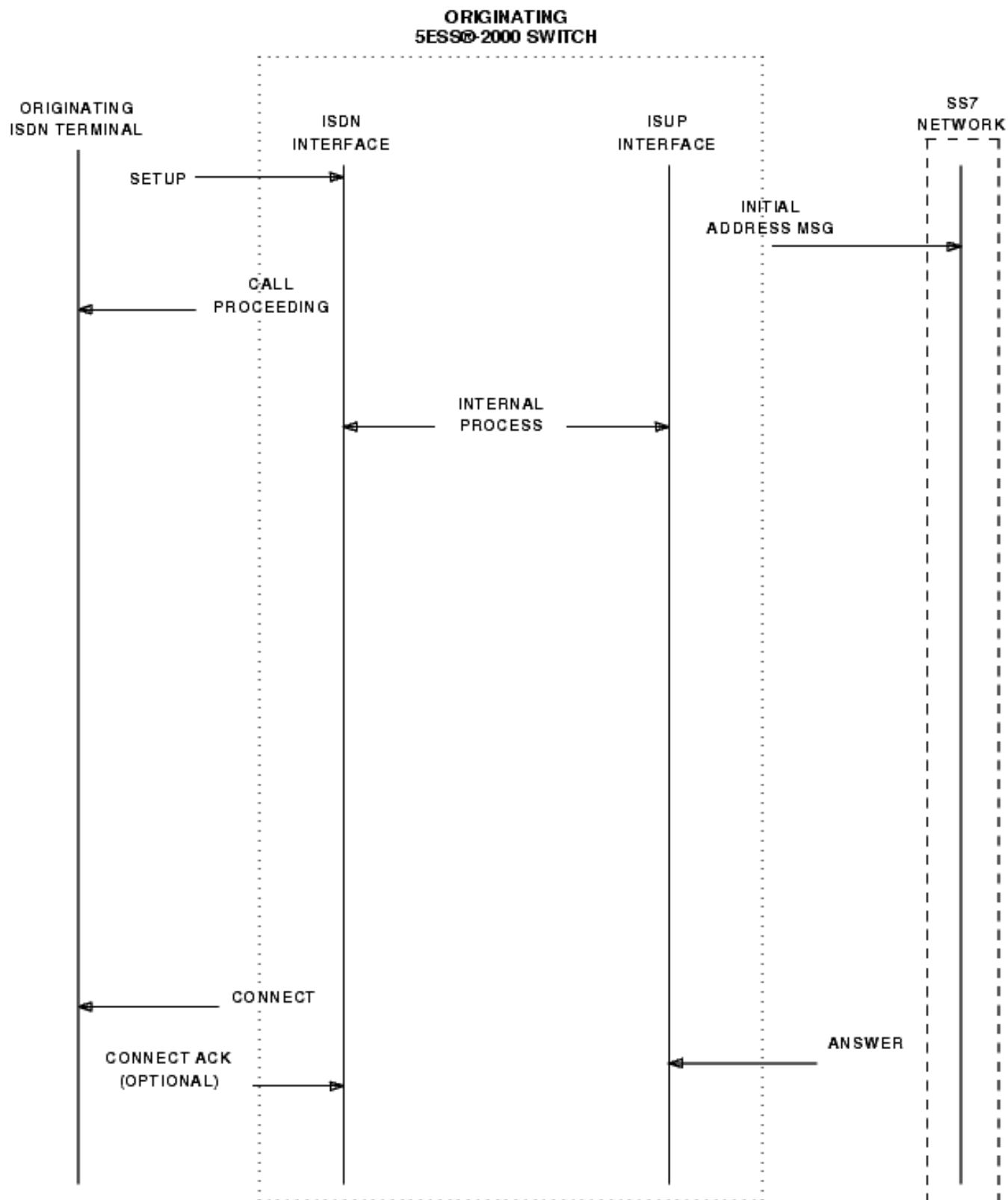


Figure 9.4-2 ISDN/ISUP Fast Connect Message Flow - Originating End

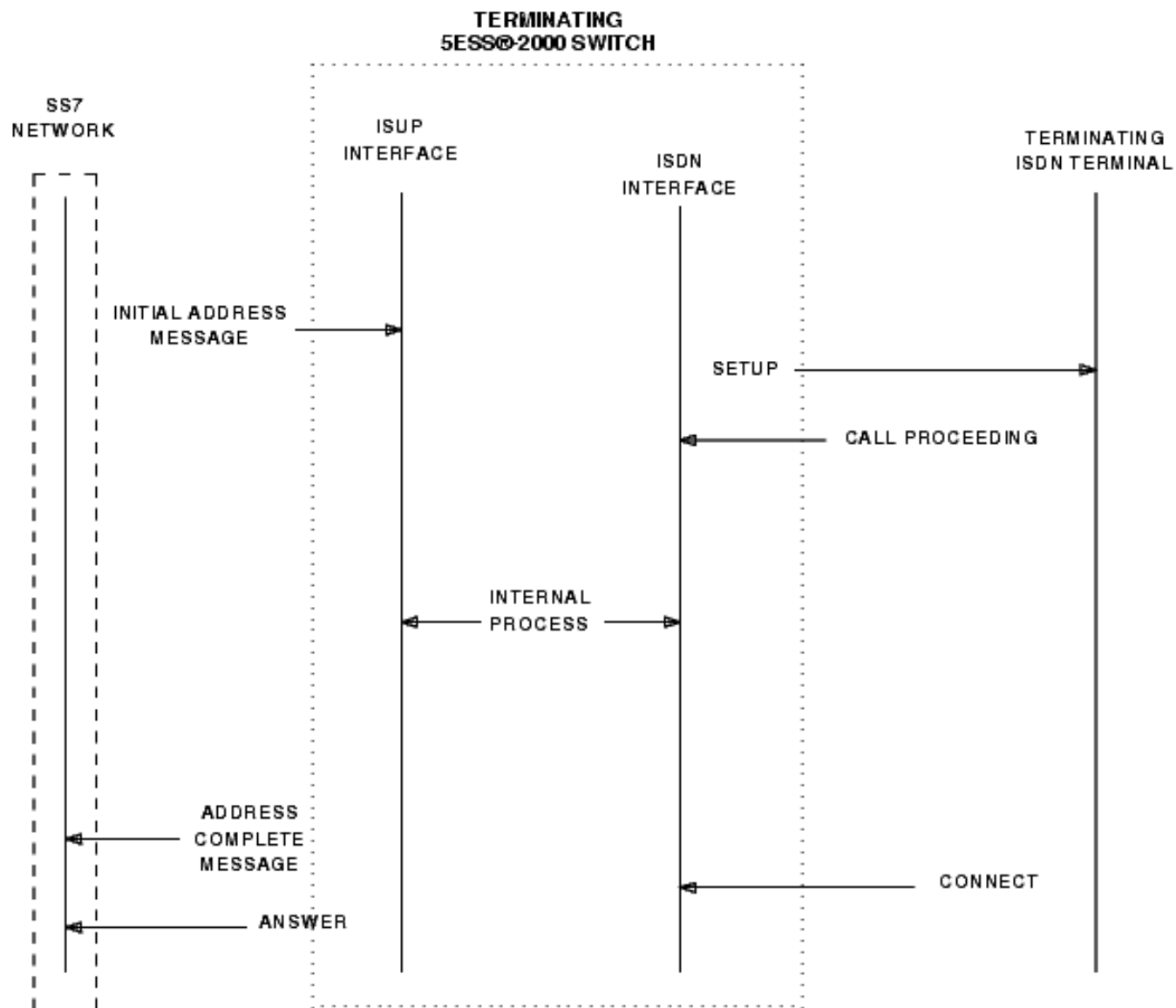


Figure 9.4-3 ISDN/ISUP Fast Connect Message Flow - Terminating End - 5E6

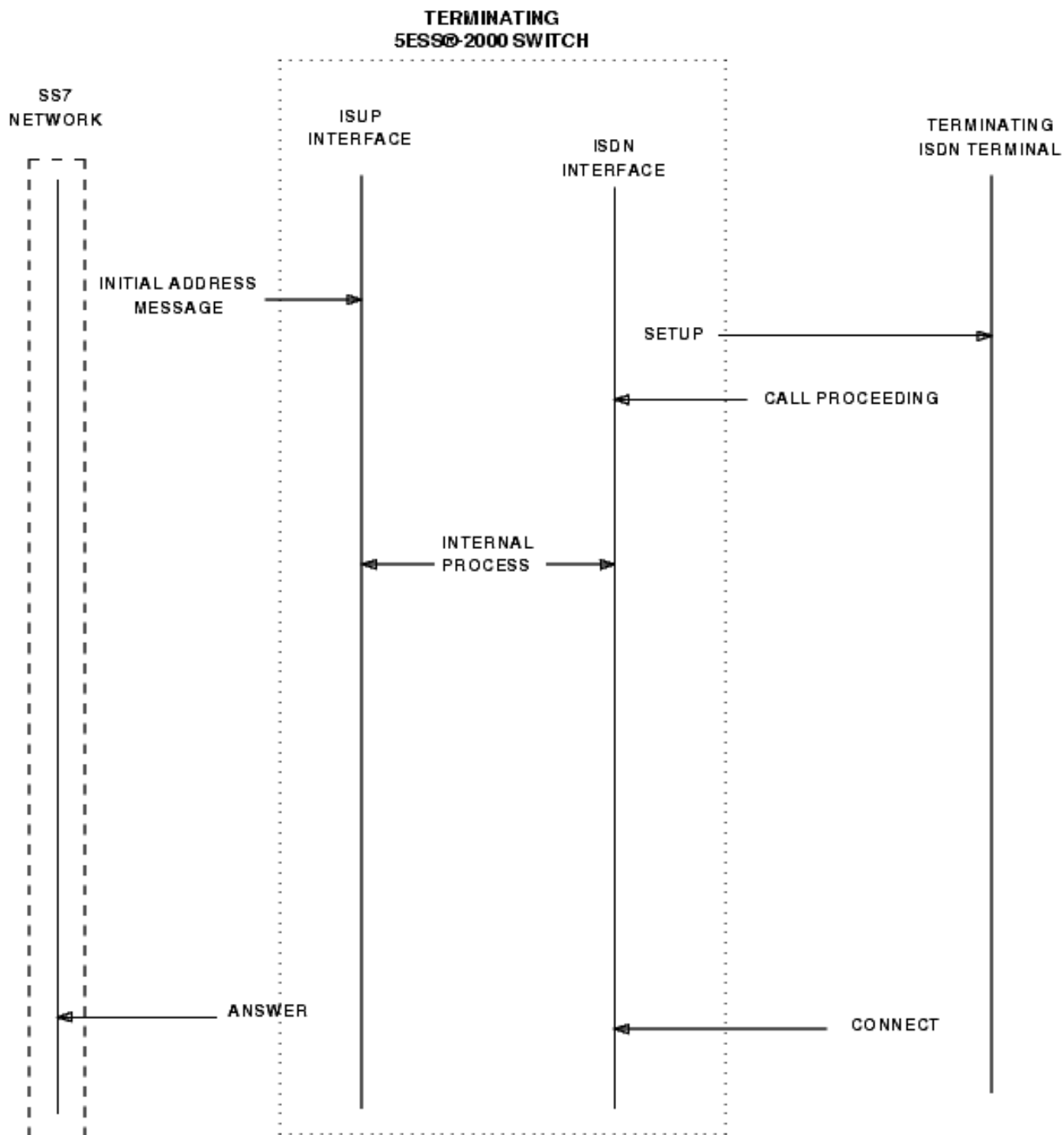


Figure 9.4-4 ISDN/ISUP Fast Connect Message Flow - Terminating End

9.4.2 Basic Call Setup And Excessive Delay Handling At The Originating Switch

Excessive ISDN call setup delay handling procedures extend the switch BRI implementation for intraswitch ISDN calls to interswitch operation. The originating exchange procedures apply to either a BRI or PRI calling party. The terminating exchange procedures apply only to a BRI called party. The actions taken by the originating interface are determined by the action of the terminating interface and the originating subscriber.

9.4.3 Basic Call Setup Excessive Call Delay Notification At The Terminating Switch With BRI

At the terminating exchange, after the SETUP message is sent to the BRI called party, Q.931 timer T303 is started. The call is expected to proceed to the next state within timer T303 (range 1 to 4 seconds, default 2.5 seconds). If the switch does not receive a CALL PROCEEDING, ALERTING, CONNECT, RELEASE COMPLETE from the outgoing circuit or an SS7 REL from the incoming circuit within the time interval T303, the call is considered encountering "excessive call setup delay" situation. The switch will attempt to set up the call until timer T310 (range 3 to 10 seconds, default 5 seconds) expires.

9.4.3.1 Excessive Call Setup Delay Handling

Tables 9.4-1 , 9.4-2 , 9.4-3 , and 9.4-4 provide an overview of the excessive call setup delay handling. The descriptions are based on the assumption that Q.931 messages received do not contain protocol errors.

Actions taken at the terminating switch are triggered by the Q.931 events occurring at the terminating BRI interface and are often based on the originating access interface (ISDN/non-ISDN) and the information transfer capability of the call (voice/data). Consider each table as a state that is entered as a result of some event. Conditions present for each table (state) are described. Possible events that change the table(s) state or exit the tables are described in the column labeled *Term. Interface BRI Only*. To move from any state to a new state, enter the current state with one of the actions in the "Term. Interface" column. How the terminating switch interprets the action, what ISUP messages are sent with the associated information, and the reactions at the originating interface are described in the other columns. If the call status column does not contain a reference to another table, the call leaves these tables and goes into normal processing and out of an excessive delay situation.

The following list of conditions applies to Tables 9.4-1 , 9.4-2 , 9.4-3 , and 9.4-4 :

- Table 9.4-1
 - SETUP is sent and T303 is started for the first time.
 - **ACM Has Not Been Sent.**
- Table 9.4-2
 - CALL Proceeding (CALL PROC) was received before the first expiration of T303; both 310 and first T303 are running.
 - **ACM Has Not Been Sent.**
- Table 9.4-3
 - T303 expired for the first time and is restarted. No CALL PROC is received. Second T303 is running.
 - **ACM Has Been Sent.**
- Table 9.4-4
 - CALL PROC was received and T303 expired for the first time. T310 is running.
(If CALL PROC was received *after* T303 first expired, the second T303 will be cancelled).
[If CALL PROC was received *before* T303 first expired (from B2 — Table 9.4-2) T303 will not be restarted].
 - **ACM Has Been Sent.**

T310 is Running.

Table 9.4-1 Call Present State

IDX	ORIG T/A ^a	ORIG. INTERFACE BRI/PRI/NON-ISDN ^{b c}	ISUP ←	TERM T/A ^a	TERM. INTERFACE BRI ONLY	CALL STATUS
A1	--	--	--	--	CALL PROC	Go to Table 9.4-2
A2	--	-- (Non-ISDN) ALERT (ISDN) PI = Inband (Voice) Signal = Audible	ACM Sub Free	Aud.	ALERT	Normal Alert Process
A3	--	-- (Non-ISDN) PROG (ISDN) PI = Inband, Delay (Voice) PI = Delay (Data) Signal = Audible	ACM Delay	Aud.	T303 1st Expiration	Delay; Go to Table 9.4-3
A4	--	-- (Non-ISDN)	ACM No Ind	Aud.	DISC/REL/REL COM Cause ≠ User Busy	Clear Term. Interface
A5	--	DISC (ISDN Data) User Busy/ Call Rej. Signal = Busy/Audible	REL User Busy/ Call Rej.	--	DISC/REL/REL COM Any Cause	Clear Term. interface
A6	busy	-- (Non-ISDN) PROG (ISDN Voice) User Busy PI = Inband Signal = Busy	REL ^d User Busy	--	DISC/REL/REL COM Cause = User Busy	Clear Term. interface
A7	aud.	PROG (ISDN Voice) Call Rej. PI = Inband Signal = Audible	REL Call Rej.	--	DISC/REL/REL COM Cause ≠ User Busy	Clear Term. interface
A8	--	-- (Non-ISDN) CONN (ISDN)	ANM	--	CONN	Fast Connect Process

Notes:

- a. Any tones and announcements indicated are provided except for ISDN data calls.
- b. PI: Progress Indicator
- c. Signal IE indicated is included only if the originating interface is BRI.
- d. For non-ISDN calling party, the switch will provide treatment based on the setting of Busy ANNC. (See Section 5.3.3.3.1.4)

Table 9.4-2 Incoming Call Proceeding State

IDX	ORIG	ORIG. INTERFACE	ISUP	TERM T/A ^a	TERM. INTERFACE	CALL

	T/A ^a	BRI/PRI/NON-ISDN b c	←		BRI ONLY	STATUS
B1	--	-- (Non-ISDN) ALERT (ISDN) PI = Inband (Voice) Signal = Audible	ACM Sub Free	Aud.	ALERT	Normal Alert Process
B2	--	-- (Non-ISDN) PROG (ISDN) PI = Inband, Delay (Voice) PI = Delay (Data) Signal = Audible	ACM Delay	Aud.	T303 1st Expiration	Delay; Go To Table 9.4-3
B3	--	-- (Non-ISDN)	ACM No Ind	Aud.	T310 Expiration	Clear Term. Interface
B4	--	DISC (ISDN Data) No User Resp Signal = Audible	REL No User Resp	--	T310 Expiration	Clear Term. Interface
B5	Aud.	PROG (ISDN Voice) No User Resp PI = Inband Signal = Audible	REL No User Resp	--	T310 Expiration	Clear Term.
B7	--	DISC (ISDN Data) User Busy/ Call Rej. Signal = Busy/Aud. ^d	REL User Busy/ Call Rej.	--	DISC/REF/REL COM Any Cause	Clear Term. Interface
B8	Busy	-- (Non-ISDN) PROG (ISDN Voice) User Busy PI = Inband Signal = Busy	REL User Busy	--	DISC/REL/REL COM Cause = User Busy	Clear Term. Interface
B9	Aud.	PROG (ISDN Voice) Call Rej. PI = Inband Signal = Audible	REL Call Rej.	--	DISC/REL/REL COM Cause ≠ User Busy	Clear Term. Interface
B10	--	-- (Non-ISDN) CONN (ISDN)	ANM	--	CONN	Fast Connect Process

Notes:

- a. Any tones and announcements indicated are provided except for ISDN data calls.
- b. PI: Progress Indicator
- c. Signal IE indicated is included only if the originating interface is BRI.
- d. Signal = busy if cause = user busy; Signal = audible if cause = call rejected.

Table 9.4-3 Delay State

IDX	ORIG T/A ^a	ORIG. INTERFACE BRI/PRI/ NON-ISDN ^{b c}	ISUP ← ^d	TERM T/A ^a	TERM. INTERFACE BRI ONLY	CALL STATUS
C1	--	--	--	Cont. Aud.	CALL PROC	Go to Table 9.4-4
C2 ^e	--	ALERT (ISDN) PI = Inband (Voice) Signal = Audible	CPG EI:Alerting	Cont. Aud.	ALERT	Delayed Alert Process
C3 ^e	--	DISC (ISDN Data) No User Resp Signal = Audible	REL No User Resp	--	T303 2nd Expiration	Clear Term. Interface.
C4 ^e	--	PROG (ISDN Voice)	CPG	Cont.	T303 2nd Expiration	Clear Term.

		PI = Inband No User Resp	El:Inband No User Resp	Aud.		Interface.
C5 ^e	--	DISC (ISDN Data) User Busy/ Call Rej. Signal = Busy/Audible	REL User Busy/ Call Rej.	--	DISC/REL/REL COM Any Cause	Clear Term. Interface.
C6 ^e	--	PROG (ISDN Voice) PI = Inband Cause Mapped	CPG El:Inband Cause Mapped	Cont. Aud.	DISC/REL/REL COM Any Cause	Clear Term. Interface.
C7	--	-- (Non-ISDN) CONN (ISDN) Signal = Tones Off	ANM	Stop Aud.	CONN	Delayed Fast Connect Process

Notes:

- Any tones and announcements already in progress are continued unless otherwise indicated.
- PI: Progress Indicator
- Signal IE indicated is included only if the originating interface is BRI.
- El: Event Indicator
- For cases C2 through C6, if the calling party is non-ISDN, no SS7 message should be sent from the terminating switch. The terminating switch should release the access interface if the call will not be completed (cases C3 through C6), continue returning audible ringing, and wait for release on the incoming circuit (calling party hang-up).

Table 9.4-4 Delayed Call Proceeding State

IDX	ORIG T/A ^a	ORIG. INTERFACE BRI/PRI/ NON-ISDN ^{b c}	ISUP ← ^d	TERM T/A ^a	TERM. INTERFACE BRI ONLY	CALL STATUS
D1 ^e	--	ALERT (ISDN) PI = Inband (Voice) Signal = Audible	CPG El:Alerting	Cont. Aud.	ALERT	Delayed Alert Process
D2 ^e	--	DISC (ISDN Data) No User Resp Signal = Audible	REL No User Resp	--	T310 Expiration	Clear Term. Interface
D3 ^e	--	PROG (ISDN Voice) PI = Inband No User Resp	CPG El:Inband No User Resp	Cont. Aud.	T310 Expiration	Clear Term. Interface
D4 ^e	--	DISC (ISDN Data) User Busy/ Call Rej. Signal = Busy/Aud. ^f	REL User Busy/ Call Rej.	--	DISC/REL/REL COM Any Cause	Clear Term. Interface
D5 ^e	--	PROG (ISDN Voice) PI = Inband Cause Mapped	CPG El:Inband Cause Mapped	Cont. Aud.	DISC/REL/REL COM Any Cause	Clear Term. Interface
D6	--	-- (Non-ISDN) CONN (ISDN) Signal = Tones Off	ANM	Stop Aud.	CONN	Delayed Fast Connect Process

Notes:

- Any tones and announcements already in progress are continued unless otherwise indicated.
- PI: Progress Indicator

- c. Signal IE indicated is included only if the originating interface is BRI.
- d. EI: Event Indicator
- e. For cases D1 through D5, if the calling party is non-ISDN, no SS7 message should be sent from the terminating switch. The terminating switch should release the access interface if the call will not be completed (cases D2 through D5), continue returning audible ringing, and wait for release on the incoming circuit (calling party hang-up).
- f. Signal = busy if cause = user busy; Signal = audible if cause = call rejected.

9.4.4 Call Failure Processing

9.4.4.1 Expiration of T(sus,r) at the Originating Exchange

When a non-ISDN called party goes on-hook, an SS7 suspend (SUS) message is sent by the terminating exchange to achieve a timed suspend/resume indicator coded "network initiated," it starts timer T(sus,r), awaiting the receipt of an SS7 RES, SS7 REL, or a Q.931 DISCONNECT. (See Table 5.6-2 for details about this timer.)

If the timer T(sus,r) expires, the originating exchange sends an SS7 REL for the outgoing circuit. The exchange also sends an access DISCONNECT message to the ISDN calling party.

9.4.4.2 Failure Encountered at the Terminating Exchange

Certain failure conditions may occur at the terminating exchange after the receipt of IAM and before sending of ACM resulting in an unsuccessful call setup.

If the first response to the first Q.931 SETUP message sent to the terminating ISDN interface contains errors that result in clearing the terminating interface, the following treatment is applied.

- If the originating access is non-ISDN, the terminating exchange follows the same procedures as if the terminating interface was network-determined busy.
- If the originating access is ISDN, an SS7 REL is sent for the incoming circuit. The cause value in the REL is set to "temporary failure (41)" and location is set to "user."

9.4.4.3 Receipt of REL at the Originating Exchange Before Connect

9.4.4.3.1 Originating Access 3.1 kHz Audio or Speech

Inband treatment is provided based on the codings of the cause indicators parameter received in the REL if the bearer capability of the calling party is either "3.1 kHz audio" or "speech."

Table 9.4-5 shows the associated inband treatment for cause values.

Table 9.4-5 Local Exchange Modification

RECEIVED CAUSE VALUE	INBAND TREATMENT
No user responding (18)	Send audible ringing
User alerting, no answer (19)	Do not send any tone
Call rejected (21)	Send audible ringing
Temporary failure (41), location "user"	Send busy tone
Temporary failure (41), location not "user"	Send reorder tone
Recovery on timer expiry (102) ^a	Do not send any tone
Protocol error cause value other than the unexpected 102	Send reorder tone
Notes:	
a. Cause 102 is not recognized in ISUP protocol, and is unexpected.	

If the cause value 102 is received, no inband tone is provided and this same cause value is used in the clearing message sent to the calling party. Note that the association of SS7 cause indicators parameter coding with an inband tone/announcement depends on the cause value only unless the cause value received is "temporary failure."

If inband treatment is provided to the calling party, a Q.931 PROGRESS message is sent to the calling party. The PROGRESS message contains a progress indicator *information element* coded "inband information or appropriate pattern now available," and location "public network serving the remote user." A cause *information element* is also included based on the coding of the cause indicators parameter in the received SS7 REL. The PROGRESS message also contains a signal *information element* with the appropriate coding. The coding of the signal *information element* is determined by the coding of the SS7 cause indicators parameter, as shown in Table 9.4-6. For cause values not shown, no signal *information element* is included in the PROGRESS message sent to the calling party.

Table 9.4-6 Coding of SS7 Cause Indicators Parameter

RECEIVED CAUSE VALUE	SIGNAL INFORMATION ELEMENT
No route to specified transit network (2)	"reorder tone on"
No route to destination (3)	"reorder tone on"
User busy (17)	"busy tone on"
No user responding (18)	"audible ringing on"
User alerting, no answer (19)	"tone off"
Call rejected (21)	"audible ringing on"
Circuit/channel congestion (34)	"reorder tone on"
Switching system congestion (42)	"reorder tone on"
Temporary failure (41), location "user"	"busy tone on"
Temporary failure (41), location not "user"	"reorder tone on"
Resources unavailable - unspecified (47)	"reorder tone on"
Recovery on timer expiry (102) ^a	"tones off"
Protocol error cause value other than the unexpected 102	"reorder tone on"
Notes:	
a. Cause 102 is not recognized in ISUP protocol, and is unexpected.	

If no inband treatment is to be provided, the originating exchange sends a Q.931 DISCONNECT to the calling party. The DISCONNECT message contains a cause *information element* mapped from the received cause indicators parameter. The DISCONNECT message may also require the inclusion of a signal *information element*, based on the coding of the cause indicator parameter. The association of the cause indicator parameter with the signal *information element* is shown in the Table 9.4-6.

9.4.4.3.2 Originating Access Restricted/Unrestricted Digital Information

If the bearer capability of the calling party is "unrestricted digital information" or "restricted digital information," no inband treatment is applied; an access DISCONNECT message is sent. The DISCONNECT message contains a cause *information element* mapped from the received cause indicators parameter and may also require the inclusion of a signal information element based on the codings of the cause indicators parameter, as shown in Table 9.4-6.

9.4.4.4 Mapping of Cause Values

9.4.4.4.1 Overview

In the 5E6 software release, the cause value and general location received in the SS7 cause indicators parameter is mapped "as is" to the Q.931 cause *information element* and vice versa. The exception, shown in "Cause Location Recoding in the 5E7 Software Release," Section 10.5.11.2, is of location codings when the SS7-supported circuit is directly connected to an IEC. The following procedures are the other exceptions to the cause transparency rule for 5E7 and later software releases.

9.4.4.4.2 Exceptions to the Transparency of Cause Values/Locations

If a cause indicators parameter is received in an SS7 message at either the originating exchange or the terminating exchange, the cause value and location are mapped to the Q.931 cause information element exactly as received, except in the following conditions:

- Location coded "local interface controlled by this signaling link" is changed to location "local local network" if the associated circuit is not directly joined to an IEC.
- Cause values received in the protocol error class (other than the unexpected 102) and also the cause value 47 ("resource unavailable - unspecified") are changed to 41 ("temporary failure").

If a cause *information element* is received in a Q.931 message, the cause value and location is mapped to the cause value and location fields of the cause indicators parameter included in the appropriate SS7 message, respectively, unless specifically stated otherwise.

9.4.5 Calling Line Identification Transport

The Calling Line Transport capability supports the Calling Number/Billing Number Delivery feature and the Calling Number Identification Service feature.

The ISUP protocol allows for interoffice transport of calling party identification information to the terminating end office. This information is transported in the calling party number parameter (CPN) and the charge number parameter (CHG) of the IAM message. The generic address parameter (GAP) is also provided for the interoffice transport of calling line information, but is not interworked to Q.931 protocol.

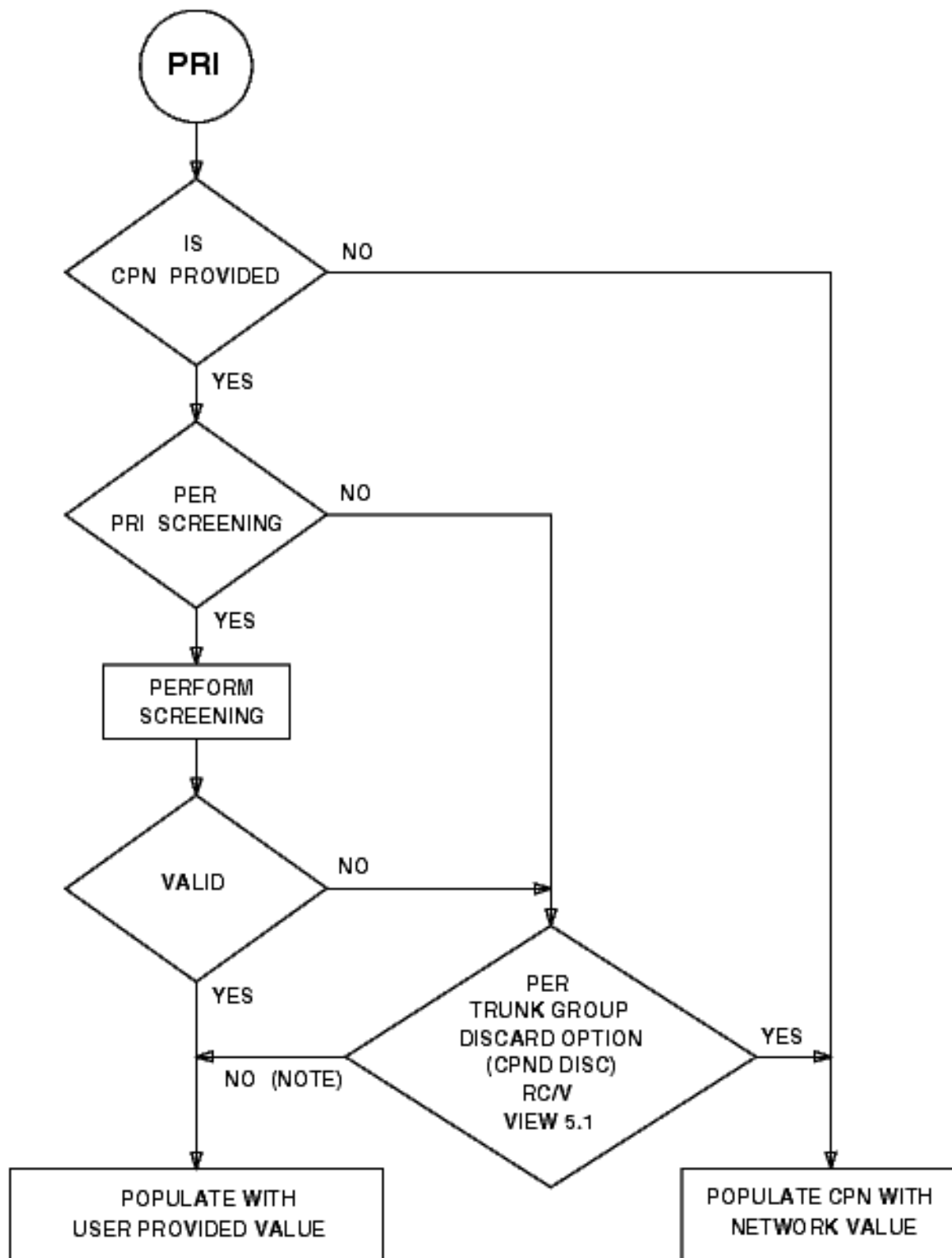
The CPN parameter is normally sent between local offices. Provisioning options are used to control the sending of calling line identification information on trunks that connect to an inter-LATA (IC) or international carrier (INC). The CPN parameter *may* or *may not* be included in the IAM depending on the subscription of the IEC to which the call is directed.

The following sections discuss controlling the sending calling line identification data and number delivery at a terminating end office.

9.4.5.1 Number Provisioning/Number Screening

Number provisioning is a subscription option which may be provided to ISDN call originators. This option allows the ISDN caller to have the ability to provide a CPN IE in a Q.931 SETUP message to the originating end office (OEO) during call setup.

If the provision required option is selected, the user must provide a valid CPN. If the subscriber has selected this option, number screening at the originating end office is performed to determine the validity of the user provided number. For the basic procedures used in number screening at the originating end office, refer to Figure 9.4-5 and Figure 9.4-6. Also, note that the GAP parameter is not generated at a switch end office.



NOTE: NO IS THE DEFAULT VALUE.

Figure 9.4-5 OEO PRI Calling Line Identification Logic

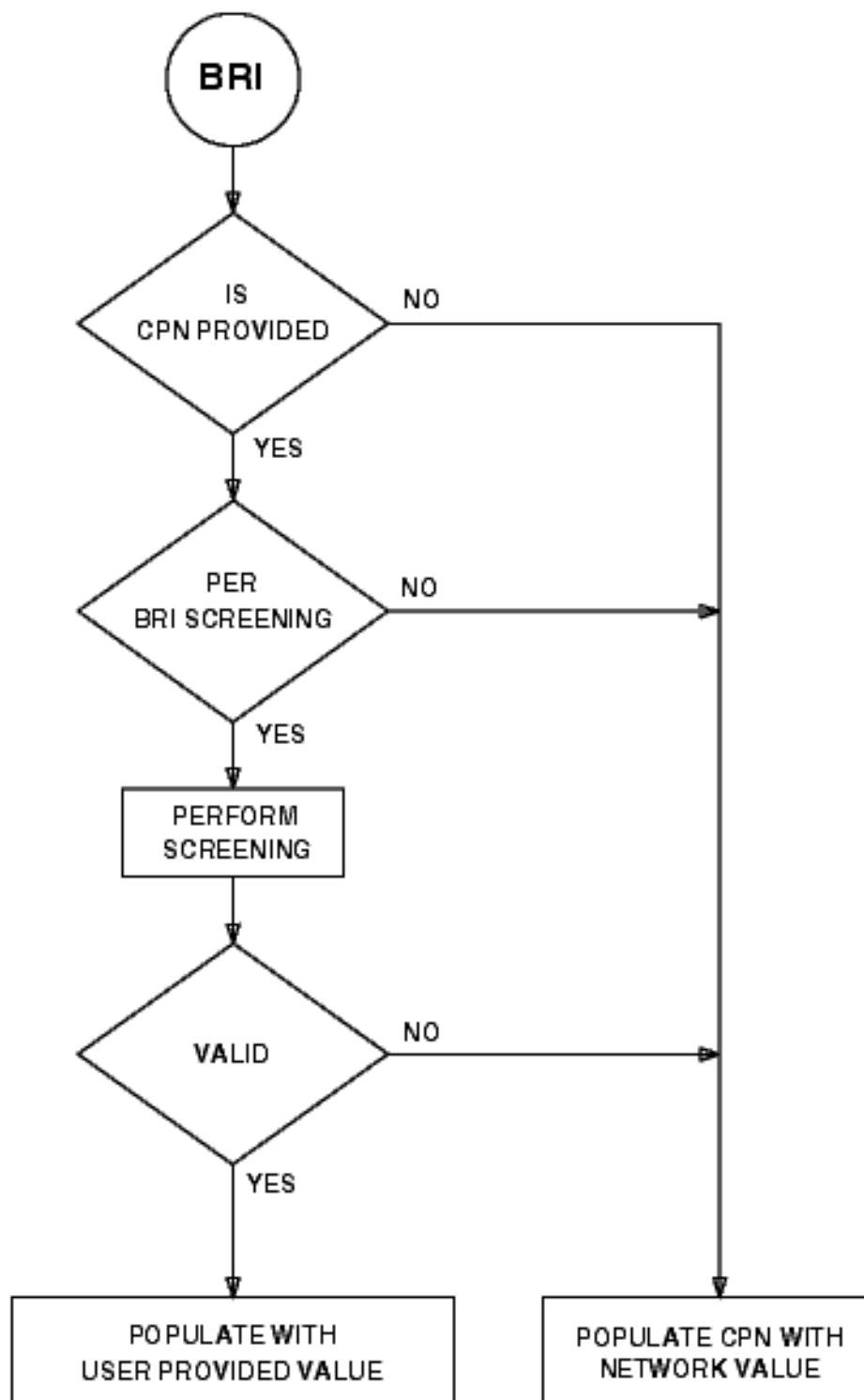


Figure 9.4-6 OEO BRI Calling Line Identification Logic

9.4.5.2 Number Privacy

Number privacy is an option available to the originating caller which maps to signaling information interpreted by the

terminating end office (TEO) to allow or inhibit the delivery of information contained in the CPN parameters to the terminating subscriber. Privacy may be invoked on a per-call or all-call basis.

9.4.5.3 Number Delivery at a Terminating End Office

Number delivery requires subscription to one or more delivery features by the terminating ISDN user. The supported ISDN number delivery features are:

- Individual Calling Line Identification (ICLID)
- Calling Party Number/Billing Number Delivery (CPN/BND)
- Calling Number Identification Service (CNIS).

9.4.5.3.1 ICLID

The ICLID feature is one of the LASS features described in "Local Area Signaling Service Features," Section 11.10 and in 235-190-130, *Local Area Signaling Service Features*.

9.4.5.3.2 CPN/BND

The CPN/BND feature is available to Custom BRI and PRI subscribers. A CPN/BND subscriber may elect to receive either: only the Calling Party Number (CPN); only the billing number (from the ISUP CHG Parameter); preferred delivery of the CPN, accepting billing number if CPN is unavailable; or preferred delivery of the billing number, accepting Calling Party Number if Billing Number is unavailable.

The CPN is interworked from the SS7 CPN parameter of a received IAM to a CPN Information Element of the Q.931 SETUP message at the time of call offering to a CPN/BND subscriber. The billing number is interworked from the SS7 CHG parameter of a received IAM to a CPN IE of the Q.931 SETUP message at the time of call offering to a CPN/BND subscriber. Only one CPN IE will be included in the SETUP message at the time of call offering. It will contain either the CPN or the billing number, depending on the subscription option chosen.

The CPN or billing number is only delivered if the originating caller has not invoked the Number Privacy option. If the "presentation status" of the CPN is "presentation restricted" (that is, "PRIVATE"), then the CPN or billing number digits are not delivered and the CPN/BND subscriber receives an indication of "CPN Presentation Restricted" in the SETUP message.

More detailed information on the CPN/BND feature is available in the 235-190-104, *ISDN Feature Descriptions* document.

9.4.5.3.3 CNIS

The Calling Number Identification Services are an expanded set of features available to National ISDN (NISDN-1) BRI users. The CNIS includes delivery of CPN, delivery of Calling Party Subaddress (CgPS), and delivery of Redirecting Number (RN) with Redirecting Reason. The delivery of CPN functions as described previously for the CPN/BND feature. The CPN is interworked from the CPN parameter of a received IAM to the CPN IE of the Q.931 SETUP message at the time of call offering to the CNIS subscriber.

Delivery of Calling Party Subaddress is a "subfunction" of CPN delivery with CNIS. An ISDN BRI user subscribing to CPN delivery will also receive CgPS delivery. The Calling Party Subaddress (CgPS) is interworked from the ATP of the received SS7 IAM to the CgPS IE of the Q.931 SETUP message at the time of call offering to the CNIS subscriber.

Delivery of Redirecting Number (RN) with Redirecting Reason is a subscription option with CNIS. An ISDN BRI user

may subscribe to RN delivery with or without subscribing to CPN delivery. An RN delivery subscriber may receive up to two RNs for a given call. The First and Last Redirecting Number(s) are interworked from the Original Called Number (OCN) and the Redirecting Number (RN) parameters of the received IAM to an RN IE(s) (two RN IEs are used if both OCN and RN are interworked) of the Q.931 SETUP message at the time of call offering to an RN delivery subscriber. Additionally, the Original Redirecting Reason is interworked from the Redirection Information Parameter (RIP) of the received IAM to the RN IE associated with the OCN. Likewise, the Last Redirecting Reason is interworked from the RIP of the received IAM to the RN IE associated with the RN.

Delivery of CPN and RN(s) are contingent on the "presentation restriction" status of the CPN or RN. If a CPN or RN is marked "presentation restricted" (that is, "PRIVATE"), the CPN or RN digits are not delivered and the CNIS subscriber receives an indication that the CPN or RN is "Restricted" in the SETUP message. Delivery of CgPS is contingent on the "nature of address" of the CPN, but not on the "presentation restriction" status of the CPN.

More detailed information on the CNIS feature is available in 235-190-104, *ISDN Feature Descriptions*.

9.5 AUTOMATIC CALL DISTRIBUTOR (ACD)/BUSINESS AND RESIDENCE CUSTOM SERVICES (BRCS) INTERWORKING

9.5.1 Definition

The ACD/BRCS Interworking feature gives end-users that serve an ACD the ability to use both existing Commercial ACD capabilities and ISDN/BRCS capabilities. End-users using customer premises equipment that complies with the Lucent Technologies Basic Rate Interface specification will have the CENTREX capabilities currently provided by ISDN /BRCS, while still taking advantage of call distribution algorithms and queuing treatment currently provided by OSPS CACD. The ACD/BRCS Interworking also removes existing restrictions that allow only certain classes of trunks to originate calls into a switch ACD.

9.5.2 Availability

This feature is available with the 5E9(1) and later software releases.

9.5.3 ISUP Call Handling For ACD/BRCS

An ISUP call that is being provided with ACD/BRCS treatment is handled as described in the following text.

9.5.3.1 Address Complete Message (ACM)

For backward notification, when a call is accepted for ACD handling an ACM is sent toward the originating exchange. The ACM is encoded to indicate that the terminating access is "non-ISDN." The ACD mechanism is not considered ISDN equipment, since inband tones and delay announcements may be provided while the call is in queue. The Backward Call Indicators parameter of the ACM message is encoded for a termination to a "non-ISDN access" (00) with a Called Party Status of "no indication" (00), and includes an Optional Backward Indicator Parameter encoded with "inband information or an appropriate pattern is now available" (1). An ATP parameter, populated with a Cause IE of "Queued" (35), is also included in the ACM.

Sending an ACM when a call first enters ACD handling, and not sending an ANM "shortly" after the ACM, may result in some networks timing-out the call due to "fraud prevention" techniques. An ACD/BRCS customer should be aware that, if answer indication (SS7 ANM or equivalent) is not received by some toll networks within a three to five minute interval, then the call will be disconnected by the toll network.

9.5.3.2 ACD Treatment

After acceptance for ACD handling, the call may be handled in many ways based on the content of the ACD office data. Answer supervision may or may not be sent. The call could be redirected to another switch using ACD interflow, a vectoring event Redirection, Delay Level Reroute, or DAA Call Forward Not Logged In Redirection (for example, mechanisms other than BRCS Call Forwarding).

NOTE: For more information on ACD handling and the dependency on ACD office data, please refer to 235-190-104, *ISDN Feature Descriptions*.

9.5.3.2.1 Answer Message

When the first ACD queuing or vectoring event that requires supervision is applied (for example; Delay Announcement, Music on Queue, Digit Collection, etc), the switch populates and sends an SS7 ANM message in the backward direction. Sending of an ANM results in billing records associated with answer supervision. Only one ANM is ever sent for the call. Once an ANM has been sent no backward messages are sent for subsequent queuing/call completion events (for example; delay announcements, music, audible), except for an REL message at the time of call clearing.

An example of a call clearing event where a REL message is sent is when an ACD/BRCS terminal, as a first response to a SETUP message, sends a DISC, REL, or REL COMP message. In this case, a REL message is sent and the terminating interface is cleared.

9.5.3.2.2 Abnormal events

After an ANM has been sent, no backward messages are sent for queued calls when an abnormal event occurs (for example, busy tone for queue full or delay exceeding level 3 threshold, route to announcement, reorder treatment). Instead, the incoming circuit is connected to the appropriate inband tone/announcement.

Abnormal Events, occurring after an ACM has been sent and prior to sending of an ANM, will result in the switch providing inband treatment appropriate to the abnormal event and sending a CPG message for ISDN originated calls EXCEPT in the following cases:

- If the outgoing side of the call is a BRI/PRI and a Q.931 access clearing message is received with cause value 19, 43, or 102, pass the cause value in a REL message to the preceding switch and idle the trunk. (Cause = 43 is unexpected in a call clearing scenario)
- If the outgoing side of the call is BRI/PRI and an incoming message (for example, ALERTING message) has already been received from the BRI/PRI, pass the cause value associated with the failure event in a REL message to the preceding switch and idle the trunk.

The CPG is encoded with an Event Indicator of "inband information or appropriate pattern now available" (3), a Presentation Restricted Indicator of "no indication" (0), and a Cause Indicator value of appropriate to the event with a location of "Public Network Serving the Remote User."

9.5.3.3 Call Handling after ACD Treatment

9.5.3.3.1 Information Elements Transport

When a call is offered to an ACD/BRCS agent, or redirected to another ISDN terminal, the user level Information Elements from the initial SETUP or IAM message are available to be delivered to the terminating ISDN. This assures that all BRCS features work transparently regardless of whether or not the call "passed through" the ACD handling.

When a call is offered to an ACD/BRCS terminal, the received contents of a Q.931 Progress or Low Layer Compatibility (LLC) IE, or the equivalent data from the SS7 ATP, is included in the SETUP message sent to the ACD/BRCS terminal. Table 9.3-1 illustrates Q.931 information element delivery.

When redirection occurs, Q.931 MA-UUI Information Elements, shown in Table 9.3-1, are preserved for delivery to the terminating ISDN terminal as appropriate.

9.5.3.3.2 Basic Call Setup Backward Signaling at the ACD Switch with BRI

9.5.3.3.2.1 Overview

At the terminating exchange, after ACD treatment, the SETUP message is sent to the BRI called party and the Q.931 timer T303 is started. The call is expected to proceed to the next state within timer T303 (range 1 to 4 seconds, default 2.5 seconds). If the switch does not receive a CALL PROCEEDING, ALERTING, CONNECT, RELEASE COMPLETE from the outgoing circuit or an SS7 REL from the incoming circuit within the time interval T303, the call is considered encountering "excessive call setup delay" situation. The switch will attempt to set up the call until timer T310 (range 3 to 10 seconds, default 5 seconds) expires.

9.5.3.3.2.2 Overview Tables

Tables 9.5-1 , 9.5-2 , 9.5-3 , and 9.5-4 provide an overview of backward signaling from the ACD switch. The descriptions are based on the assumption that Q.931 messages received do not contain protocol errors.

If an ANM message was already sent for the call, no backward message is returned for the received CONNect.

Actions taken at the terminating switch are triggered by the Q.931 events occurring at the terminating BRI interface and are often based on the originating access interface (ISDN/non-ISDN). Consider each table as a state that is entered as a result of some event. Conditions present for each table (state) are described. Possible events that change the table(s) state or exit the tables are described in the column labeled *Term. Interface BRI Only*. To move from any state to a new state, enter the current state with one of the actions in the "Term. Interface" column. How the terminating switch interprets the action, what ISUP messages are sent with the associated information, and the reactions at the originating interface are described in the other columns. If the call status column does not contain a reference to another table, the call leaves these tables and goes into normal processing and out of an excessive delay situation.

The following list of conditions applies to Tables 9.5-1 , 9.5-2 , 9.5-3 and 9.5-4 :

- Table 9.5-1
 - SETUP is sent and T303 is started for the first time.
 - **ANM Has Not Been Sent.**
- Table 9.5-2
 - CALL Proceeding (CALL PROC) was received before the first expiration of T303; both 310 and first T303 are running.
 - **ANM Has Not Been Sent.**
- Table 9.5-3
 - T303 expired for the first time and is restarted. No CALL PROC is received. Second T303 is running.
 - **ANM Has not Been Sent.**
- Table 9.5-4
 - CALL PROC was received and T303 expired for the first time. T310 is running.
(If CALL PROC was received *after* T303 first expired, the second T303 will be cancelled).
[If CALL PROC was received *before* T303 first expired (from B2 — Table 9.5-2) T303 will not be restarted].
 - **ANM Has Not Been Sent.**
 - T310 is Running.**

Table 9.5-1 ACD Call Present State

IDX	ORIG T/A ^a	ORIG. INTERFACE BRI/PRI/ NON-ISDN ^{b c}	ISUP ←	TERM T/A ^a	TERM. INTERFACE BRI ONLY	CALL STATUS

A1	--	--	--	--	CALL PROC	Go to Table 9.5-2
A2	--	-- (Non-ISDN)	--	Aud.	ALERT	Normal Alert Process
A3	--	ALERT (ISDN) PI = Inband (Voice) Signal = Audible	CPG BCI. CdPstat=Sub Free isdn_term=Y	Aud.	ALERT	Normal Alert Process
A4	--	-- (Non-ISDN)	--	Aud.	T303 1st Expiration	Delay; Go to Table 9.5-3
A5	--	PROG (ISDN) PI = Inband, Delay (Voice)	CPG Delay	Aud.	T303 1st Expiration	Delay; Go to Table 9.5-3
A6	--	-- (Non-ISDN)	--	Aud.	DISC/REL/ REL COM Cause ≠ User Busy	Clear Term. Interface
A7	--	-- (Non-ISDN)	--	Busy	DISC/REL/ REL COM Cause = User Busy	Clear Term. interface
A8	--	-- (Non-ISDN)	--	Busy	DISC/REL/ REL COM	Clear Term. interface
A9	--	PROG (ISDN Voice) User Busy PI = Inband Signal = Busy	CPG Cause = User Busy	Busy	DISC/REL/ REL COM Cause = User Busy	Clear Term. interface
A10	--	PROG (ISDN Voice) Call Rej. PI = Inband Signal = Audible	CPG Cause = Call Rej.	Aud.	DISC/REL/ REL COM Cause ≠ User Busy	Clear Term. interface
A11	--	-- (Non-ISDN) CONN (ISDN)	ANM BCI.isdn_term = Y	--	CONN	Fast Connect Process

Notes:

- a. Any tones and announcements indicated are provided except for ISDN data calls.
- b. PI: Progress Indicator
- c. Signal IE indicated is included only if the originating interface is BRI.
- d. party, the switch will provide treatment based on the setting of Busy ANNC. (See Section 5.3.3.3.1.4)

Table 9.5-2 ACD Incoming Call Proceeding State

IDX	ORIG T/A ^a	ORIG. INTERFACE BRI/PRI/ NON-ISDN ^{b c}	ISUP ←	TERM T/A ^a	TERM. INTERFACE BRI ONLY	CALL STATUS
B1	--	-- (Non-ISDN)	--	Aud.	ALERT	Normal Alert Process
B2	--	ALERT (ISDN) PI = Inband (Voice) Signal = Audible	CPG BCI. CdPstat = subfree isdn_term = Y	Aud.	ALERT	Normal Alert Process

B3	--	-- (Non-ISDN)	--	Aud.	T303 1st Expiration	Delay; Go to Table 9.5-3
B4	--	PROG (ISDN) PI = Inband, Delay (Voice) Signal = Audible	CPG Delay	Aud.	T303 1st Expiration	Delay; Go to Table 9.5-3
B5	--	-- (Non-ISDN)	--	Aud.	T310 Expiration	Clear Term. Interface
B6	--	PROG (ISDN Voice) No User Resp PI = Inband Signal = Audible	CPG No User Resp	Aud	T310 Expiration	Clear Term.
B7	--	-- (Non-ISDN)	--	Busy	DISC/REL/ REL COM Cause = User Busy	Clear Term. Interface
B8	--	-- (Non-ISDN)	CPG	Busy	DISC/REL/ REL COM	Clear Term.
B9	--	PROG (ISDN Voice) User Busy PI = Inband Signal = Busy	CPG User Busy	Busy	DISC/REL/ REL COM Cause = User Busy	Clear Term. Interface
B10	--	-- (Non-ISDN)	--	Aud	DISC/REL/ REL COM Cause User Busy	Clear Term. Interface
B11	--	PROG (ISDN Voice) Call Rej. PI = Inband Signal = Audible	CPG Call Rej.	Aud	DISC/REL/ REL COM Cause ≠ User Busy	Clear Term. Interface
B12	--	-- (Non-ISDN) CONN (ISDN)	ANM BCI. isdn_term = Y	--	CONN	Fast Connect Process

Notes:

- a. Any tones and announcements indicated are provided except for ISDN data calls.
- b. PI: Progress Indicator
- c. Signal IE indicated is included only if the originating interface is BRI.
- d. Signal = busy if cause = user busy; Signal = audible if cause = call rejected.

Table 9.5-3 ACD Delay State

IDX	ORIG T/A ^a	ORIG. INTERFACE BRI/PRI/ NON-ISDN ^{b c}	ISUP ← ^d	TERM T/A ^a	TERM. INTERFACE BRI ONLY	CALL STATUS
C1	--	--	--	Cont. Aud.	CALL PROC	Go to Table 9.5-4
C2 ^e	--	ALERT (ISDN) PI = Inband (Voice) Signal = Audible	CPG BCI. isdn_term = Y EI:Alerting	Cont. Aud.	ALERT	Delayed Alert Process
C3 ^e	--	PROG (ISDN Voice)	CPG	Cont.	T303 2nd Expiration	Clear Term.

		PI = Inband No User Resp	El:Inband No User Resp	Aud.		Interface
C4 ^e	--	PROG (ISDN Voice) PI = Inband Cause Mapped	CPG El:Inband Cause Mapped	Cont. Aud.	DISC/REL/REL COM Any Cause	Clear Term. Interface
C5	--	-- (Non-ISDN) CONN (ISDN) Signal = Tones Off	ANM BCI. isdn_term = Y	Stop Aud.	CONN	Delayed Fast Connect Process

Notes:

- Any tones and announcements already in progress are continued unless otherwise indicated.
- PI: Progress Indicator
- Signal IE indicated is included only if the originating interface is BRI.
- El: Event Indicator
- For cases C2 through C4, if the calling party is non-ISDN, no SS7 message should be sent from the terminating switch. The terminating switch should release the access interface if the call will not be completed (cases C4 through C6), continue returning audible ringing, and wait for release on the incoming circuit (calling party hang-up).

Table 9.5-4 ACD Delayed Call Proceeding State

IDX	ORIG T/A ^a	ORIG. INTERFACE BRI/PRI/ NON-ISDN ^{b c}	ISUP ← ^d	TERM T/A ^a	TERM. INTERFACE BRI ONLY	CALL STATUS
D1 ^e	--	ALERT (ISDN) PI = Inband (Voice) Signal = Audible	CPG El:Alerting	Cont. Aud.	ALERT	Delayed Alert Process
D2 ^e	--	PROG (ISDN Voice) PI = Inband No User Resp	CPG El:Inband No User Resp	Cont. Aud.	T310 Expiration	Clear Term. Interface
D3 ^e	--	PROG (ISDN Voice) PI = Inband Cause Mapped	CPG El:Inband Cause Mapped	Cont. Aud.	DISC/REL/ REL COM Any Cause	Clear Term. Interface
D4	--	-- (Non-ISDN) CONN (ISDN) Signal = Tones Off	ANM BCI. isdn_term = Y	Stop Aud.	CONN	Delayed Fast Connect Process

Notes:

- Any tones and announcements already in progress are continued unless otherwise indicated.
- PI: Progress Indicator
- Signal IE indicated is included only if the originating interface is BRI.
- El: Event Indicator
- For cases D1 through D2, if the calling party is non-ISDN, no SS7 message should be sent from the terminating switch. The terminating switch should release the access interface if the call will not be completed (cases D2 through D3), continue returning audible ringing, and wait for release on the incoming circuit (calling party hang-up).
- Signal = busy if cause = user busy; Signal = audible if cause = call rejected.

10. ISUP NETWORK INTERCONNECT

10.1 AVAILABILITY

NOTE: The 5E9(1) and later software releases support the Feature Group D (FGD) Carrier Identification Code (CIC) Expansion feature. This feature expands the CIC (represented in the text as XXX) from three to four digits. Throughout this section, when CIC is encountered it should be read as either XXX or XXXX. See "Feature Group D (FGD) Carrier Identification Code (CIC) Expansion," Section 10.5.6 for more detail.

Integrated Services Digital Network User Part (ISUP) Network Interconnect (NI) capability is provided for the 5ESS®-2000 switch with the 5E6 and later software releases.

The 5E7 software release enhanced the Network Interconnect (NI) capabilities available with the 5E6 software release.

10.2 DEFINITIONS

10.2.1 Definitions Introduction

The NI allows interconnection of the various Signaling System 7 (SS7) networks used by the LECs, IECs, the government, and private companies of North America. This provides the capabilities needed for advanced telecommunications and transparent operation of network services. End-to-end ISUP eliminates the signaling deficiencies of traditional inband signaling.

This feature is independent of the signaling network architecture. However, ISUP protocol uses the CCS signaling network for message transport via the message transfer part (MTP) layer of the ISUP protocol. Figure 10-1 shows the typical network interconnect architecture.

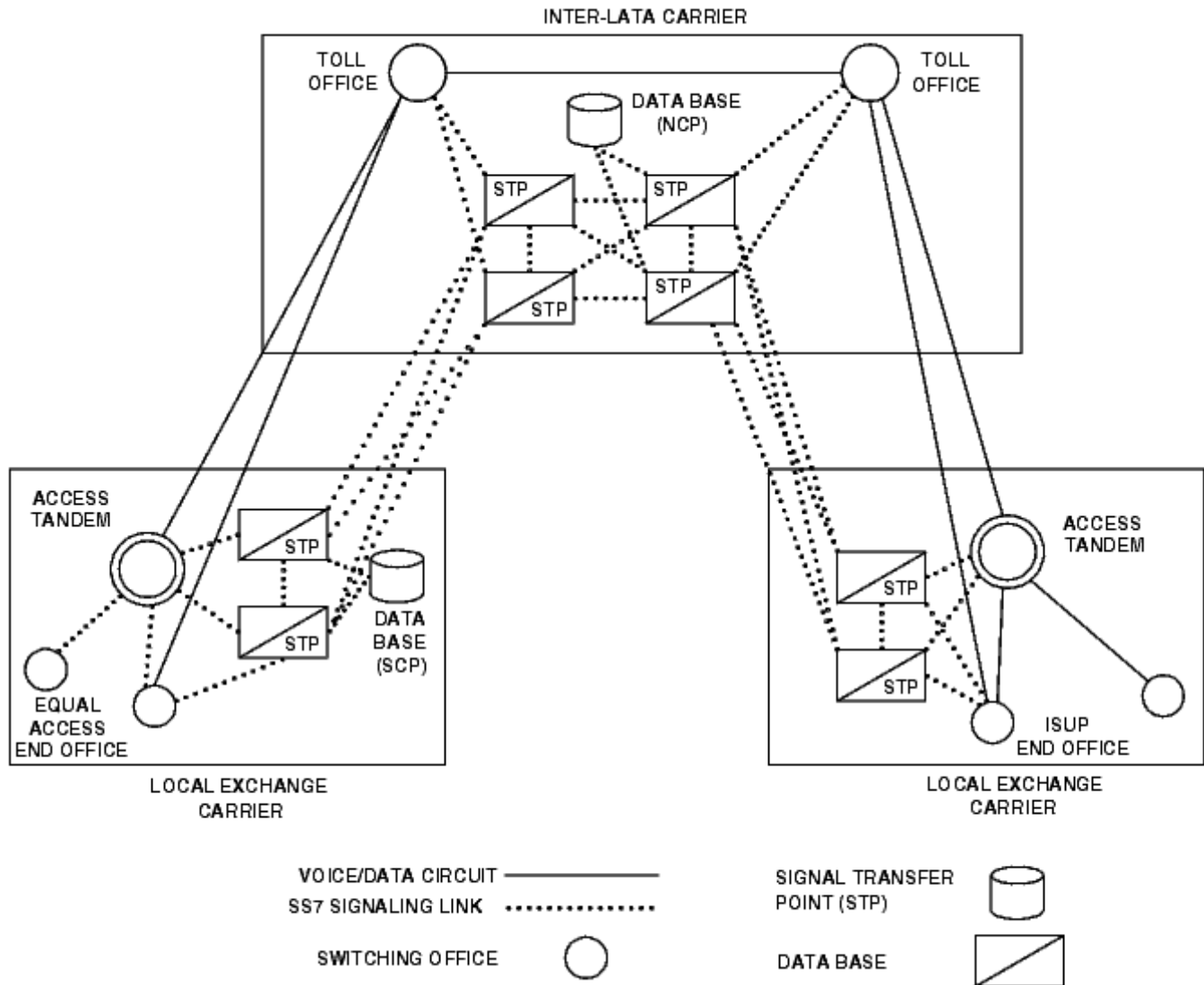


Figure 10-1 Network Interconnect Architecture

10.2.2 Switching Offices

The switching offices involved in ISUP network interconnect are referred to in this section by their functional title. The following are the definitions of those functional titles:

- **End Office (EO)**

This is the local exchange carrier (LEC) switch that serves a customer for a call. The end office must support customer lines as well as trunks to an access tandem office or inter-LATA/international carrier toll office. The originating end office is the office serving the calling party. The terminating end office serves the called party.

- **Access Tandem (AT)**

This is an LEC switch that allows calls from several end offices to be consolidated for transport to an IEC. The access tandem also accepts calls from the IEC and directs them to the end offices. The originating access tandem serves the originating end offices and the terminating access tandem serves the terminating end offices. If a switch serving as an access tandem terminates customer lines, the switch is considered the end

office for calls to and from those lines.

- **Service Switching Point (SSP)**

This is an end office or access tandem with access to a service control point for processing number service calls. If an access tandem serves as a service switching point, the signaling between the end office and the access tandem does not distinguish between intranetwork and internetwork calls and, therefore, is not addressed by this feature. Instead, the service switching point (SSP) office identifies calls requiring IEC handling and is, therefore, regarded as the end office relative to the network interconnect feature.

- **Toll Office (TO)**

This is any switch within an IEC, or consolidated carrier network. The originating toll office is the first IEC office to which a call is routed from the originating LATA. The terminating toll office is the last IEC office through which a call is routed before entering the LATA in which the called number is located.

10.2.3 Call Types

There are two types of calls that originate and/or terminate within an LEC network and are transported by an IEC.

- **Domestic Calls**

Domestic calls originate and terminate within world zone 1. The domestic calls are divided into calls within the continental U.S. and international region calls. International region calls are calls between the continental U.S. and a region within world zone 1 outside the continental U.S. (such as, Hawaii, Alaska, Canada, parts of Mexico, etc.).

- **International Calls**

International calls are calls between the continental U.S. and a point outside world zone 1 that are transmitted via the international network. These calls may originate and terminate in either the continental U.S. or in a location outside of world zone 1.

10.2.4 Carrier Types

There are three types of long distance carriers referred to in this section.

- **Inter-LATA Carrier (IC)**

This is a telecommunications carrier that handles traffic between the LATAs. The inter-LATA carrier (IC) only handles domestic calls. Some ICs are not able to handle calls to international regions outside the continental U.S. Customers may have to access another carrier for such calls.

- **International Carrier (INC)**

This is a telecommunications carrier that handles international calls. Some international carriers can also handle domestic calls to international regions (within world zone 1). An international carrier (INC) cannot handle domestic calls within the continental U.S.

- **Consolidated Carrier**

This is a telecommunications carrier that handles a mix of domestic and international calls.

- **Interexchange Carrier (IEC)**

An Interexchange Carrier can be any of the previous.

Another type of carrier referred to in this section is a Local Exchange Carrier (LEC). A LEC is a Bell Operating Company (BOC) or Independent Telephone Company (ITC) which handles intra-LATA calls and provides access to Interexchange Carriers.

10.2.5 Signaling Types

There are two types of signaling protocols referred to in this section for call processing through the LEC and toll networks. Both of these signaling types may be used in a single call between networks.

- ***Inband Signaling***

This is a signaling protocol in which the signaling information is conveyed through the same facility that is used for the voice and data transmission path. This includes multifrequency and dial pulse signaling. Equal access inband signaling uses multifrequency signaling and supports equal access arrangements. Traditional inband signaling supports traditional (non-equal) access and all egress arrangements.

- ***ISUP***

This is a Common Channel Signaling protocol in which the signaling information is conveyed through facilities separate from those used for the voice and data transmission path.

10.2.6 Voice And Data Transmission Facilities

In this document, the transmission paths for voice and data calls through the networks are referred to as trunk groups or circuit groups. No attempt is made to identify the physical makeup of these transmission paths.

10.3 FEATURE BENEFITS

10.3.1 Basic Call Setup

With the 5E6 software release, the LEC and IECs could set up intranetwork calls using the ISUP protocol. Calls that crossed between networks still needed to use inband signaling and ISDN features, such as calling party identification, could be provided by the LEC only on intra-LATA calls. The intra-LATA version of the ISUP feature did not provide the additional information needed to support equal access arrangements, such as Feature Group D and Feature Group B services to IECs.

The ISUP Network Interconnect feature integrates the basic ISUP call setup capabilities and the equal access arrangements currently available using equal access multifrequency (EAMF) inband signaling. This feature provides the necessary enhancements to ISUP to support equal access calls from the LEC to an IEC. Additional ISUP messages and parameters are used to support these internetwork interfaces.

10.3.2 Facility And Service Identification

The current EAMF inband signaling protocol is unable to convey the transmission requirements for a call. In addition, it does not provide the means to explicitly identify the service associated with a call except where the service is identified by the called number. Therefore, current network interconnect arrangements rely on the use of dedicated facilities for the identification of facility and service requirements. ISUP protocol provides the capability for more sophisticated facilities and characteristics necessary for a call. This allows different types of traffic to share the facilities between LECs and IEC; thus, alleviating the less efficient use of dedicated facilities.

10.3.3 ISDN Features And Services

10.3.3.1 ISDN Features And Services Introduction

In addition to supporting equal access call arrangements, this feature also supports ISDN features previously available only on intranetwork ISUP calls. These include 64 kb/s digital data calls, Calling Party Identification, and Q.931 Information Element Transport.

10.3.3.2 Q.931 Information Element Transport

10.3.3.2.1 Q.931 Information Element Transport Introduction

The "Q.931 Information Element Transport (ATP)," Section 5.4.1.2.1 discusses Q.931 information element transport in detail. More information on Q.931/ISUP interworking can be found in "Q.931/ISUP Interworking Feature Description," Section 9.2.3. The information in this section addresses issues uniquely related to Network Interconnect.

10.3.3.2.2 Message Associated User-to-User Information (MA-UUI)

In the 5E6 software release, if both calling and called parties are ISDN subscribers, it is possible for a calling/called party to transfer user-to-user information through the signaling network to a called/calling party during the setup and clearing phases of a call. If the user provides it, *user-to-user information* is included in the IAM, ACM, ANM, and REL messages for the 5E6 software release.

The access transport parameter (discussed in "User-To-User Information Transport," Section 9.3) transports the Q.931 information elements between ISDN customer interfaces. The combination of these two parameters is referred to as Message Associated User-to-User Information. In the 5E6 software release, MA-UUI could be restricted on trunks groups (See Table 5.5-1, MAUUI RSTCT) directly connected to the carrier either on access from the LEC network to the IEC network or on egress from the IEC to the LEC network. One restriction indicator was used in 5E6 for the combined ATP and UUI parameters considered Message Associated User-to-User Information. The length of MA-UUI cannot exceed 64 octets of data in 5E6 and earlier software releases. If a switch receives a message containing MA-UUI which is to be routed over a trunk directly connected to an IEC, outgoing screening is performed to determine whether to drop the MA-UUI. Similarly, if a message is received on egress over an incoming trunk directly connected to an IEC, incoming screening is performed to determine whether the switch will drop the incoming MA-UUI.

10.3.3.2.3 5E7 and Later Software Releases

The 5E7 and later software releases decouple the access transport parameter from the *user-to-user information* parameter giving higher priority to the access transport parameter. Each parameter may be up to 131 octets (including parameter name and length octets). This feature also includes changes to internetwork screening at local offices.

The following is a list of Q.931 information elements transport and user-to-user enhancements:

- Per-IEC subscription to *user-to-user information* and access transport parameter (separate subscriptions):

This capability is intended to replace the Phase 1 outgoing per-circuit group screening. Phase 2 EOs and ATs should discontinue use of outgoing screening. To minimize transition, the default setting for IEC subscription to each of these parameters is "not subscribed" which is consistent with the default of "do not pass" for Phase 1 outgoing screening.

- Incoming screening of *user-to-user information* and access transport parameter from IEC (separate screening) (See Table 5.5-1, ATP IC RSTCT and UUI IC RSTCT):

Phase 1 used a single combined per-circuit group indicator for incoming screening for *user-to-user information* and access transport parameter. Phase 2 EOs and ATs must provide separate indicators which can be

administered independently. To minimize transition, the default setting for the two Phase 2 circuit group indicators is "discard" which is consistent with the default of "discard" for the single Phase 1 indicator.

10.3.3.3 Carrier Selection Information (CSI)

The CSI parameter is included, if subscribed, in the IAM on a per-IEC basis (See Table 5.5-1, CSI SUBSC). The CSI field is coded as follows:

- Selected Carrier Identification Code (CIC) presubscribed and not input by calling party.
 - If the calling party is presubscribed to the IEC and did not dial 10XXX.
- Selected CIC presubscribed and input by calling party
 - If the calling party is presubscribed to the IEC and dialed 10XXX where XXX is the CIC of the IEC.
- Selected CIC not presubscribed and input by the calling party
 - If the calling party is not presubscribed to the IEC and dialed 10XXX where XXX is the CIC of the IEC.

Table 10-1 shows cases where the CSI parameter is sent in the outgoing IAM and the values used in the parameter.

Table 10-1 CSI Parameter Coding

Dialed Digits	Line/Q.931 Presub- scribed Carrier Present	Trunk Group Presub- scribed Carrier Present	Default Office Presub- scribed Carrier Present	CSI Sub- scribed	CIC Match	CSI Coding
10XXX not dialed	Y	DC	DC	Y	-	1
10XXX not dialed	N	Y	DC	Y	-	1
10XXX not dialed	N	N	Y	Y	-	1
10XXX not dialed	N	N	N	Y/N	-	call fails
10XXX+DN	Y	DC	DC	Y	Y	2
10XXX+DN	N	Y	DC	Y	Y	2
10XXX+DN	N	N	Y	Y	Y	2
10XXX+DN	Y	DC	DC	Y	N	4
10XXX+DN	N	Y	DC	Y	N	4
10XXX+DN	N	N	Y	Y	N	4
10XXX+DN	N	N	N	Y	N	4 ^a
DC	DC	DC	DC	N	DC	no CSI sent
Notes:						
a. This covers the case where no default CIC is available.						

If the call is processed as a Service Switching Point (SSP) call, or dialed using SAC codes (*800, 900, etc.), a CSI parameter is **not** included in the IAM.

10.3.3.4 Calling Line Identification (CLID)

10.3.3.4.1 Calling Line Identification (CLID) Introduction

Calling line identification (CLID) is a basic capability available to both analog and ISDN interfaces. The 5E6 software release provided for the transport of a single Calling Party Number (CPN), in addition to automatic number

identification (ANI), also known as, charge parameter (CHG). The 5E7 software release extends this capability to provide for the transport of one or two CPNs where one is network validated and the other, if applicable, is not.

The network validated CPN is transported in the CPN parameter while the other CPN is transported in the generic address parameter (GAP).

NOTE: Non validated CPNs carried in the GAP parameter are not generated at a switch end office but will be passed as received at a tandem switch. The GAP parameter is also not interworked at a terminating end office.

10.3.3.4.2 Originating End Office

The CPN parameter is always generated by the originating exchange and carried in the IAM on intra-LATA calls. For inter-LATA and international calls, the CPN parameter is included in the outgoing IAM on a per-IEC subscription basis. The CPN parameter may only transport network validated numbers.

10.3.3.4.3 Tandem Office

On receipt of a CPN parameter in the IAM, the tandem office passes the CPN parameter to the succeeding exchange in the outgoing IAM without any modifications.

On receipt of one or more generic address parameters, the tandem office does the following:

If the received GAP has a type of address of "User-provided, failed screening" or "User-provided, not screened," it is passed in the GAP parameter. A received GAP with any other type of address is passed as an unrecognized parameter. Note that only the first instance of a GAP of the user-provided type is passed in the GAP, any other subsequent GAPs of the user-provided type are passed as unrecognized.

Any per-IEC CPN subscription options (See Table 5.5-1, C/N SUBSC), which controls the sending of the GAP, apply only to the recognized GAP. Unrecognized parameters, including GAPs of type other than "user-provided," are passed unchanged.

NOTE: GAP is not sent from an OEO switch.

10.3.3.4.4 Terminating End Office

On receipt of an IAM with the CPN parameter at the terminating exchange, the CPN carried in the CPN parameter may be provided to the called party based on the subscription options of the called party and the setting of the presentation restriction indicator field of the number, or the number may be passed to other feature software requiring its use.

10.3.3.5 Charge Number (CHG) Parameter

10.3.3.5.1 Originating End Office

As an originating end office, the switch always generates the charge number (CHG) parameter in the IAM for intra-LATA calls. The CHG parameter is included in the IAM by the switch on a per-IEC basis for inter-LATA and international calls (See Table 5.5-1, ANI IND).

10.3.3.5.2 Tandem Office

If the CHG parameter is received in the incoming IAM at an intermediate exchange, it is passed in the outgoing IAM without modification.

10.3.3.5.3 Terminating End Office

If the received IAM at a terminating switch contains the CHG parameter, this number may be interworked to the Q.931 CPN IE, depending on feature software.

10.4 DEPENDENCIES AND LIMITATIONS

10.4.1 Dependencies

The 5E7 software release builds upon the Network Interconnect Phase 1 feature (5E6 software release) and is dependent upon the following for an end-to-end ISUP call:

- LEC access tandems supporting ISUP NI must be upgraded to the 1AE11, 4E14, and 5E6 software release (or TR-394 compatible software release from another vendor).
- LEC originating end offices must be upgraded to 1AE11 or 5E6 (or TR-394 compatible software release).
- LEC terminating end offices not directly connected to IECs may be an earlier ISUP capable software release.

10.4.2 Limitations

10.4.2.1 Operator Systems Signaling

ISUP protocol does not support supplemental signaling, operator control disconnect, or signaling between operator systems. Supplemental signaling includes coin control signals between the coin phones and the operator. Multifrequency inband signaling continues to be used for calls from coin phones, calls requiring operator assistance, calling card calls, and calls involving the LEC operator.

ISUP protocol supports delivery of operator requested calls from the LEC to the IEC when an LEC operator system is not required. IECs may choose to receive operator calls over the ISUP network with the understanding that the operator system signaling is not available for such calls.

10.4.2.2 Protocol Messages and Parameters

Certain ISUP messages and parameters are restricted to internetwork use. See Table 5.1-1 in "ISUP Messages and Parameters," Section 5.1 for a list of all ISUP messages, parameters, and any network limitations.

10.5 FEATURE OPERATION

10.5.1 ISUP End Office To ISUP Toll Office Direct Circuit

10.5.1.1 Message Flow

A call between the LEC and the IEC may be over a direct circuit or via an access tandem. This applies to both domestic and international calls. An originating international call is distinguished from an originating domestic call by the nature of address indicator within the called party number parameter included in the IAM sent to the IEC. A terminating international call is distinguished from a terminating domestic call by the national/international call indicator in the forward call indicator parameter.

Figure 10-2 illustrates the exchange of ISUP messages between the end office and the toll office for call setup over a direct circuit.

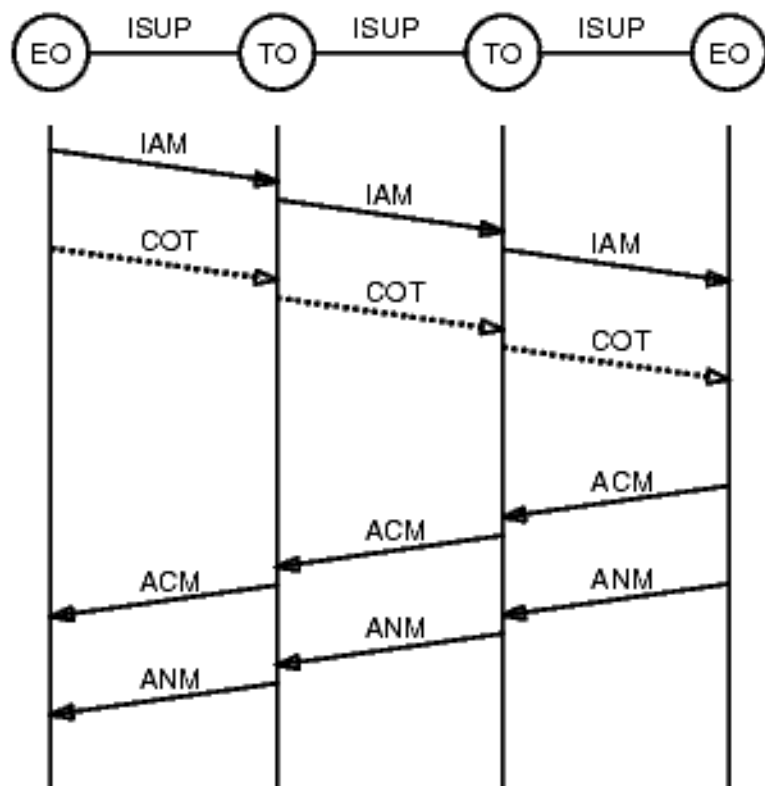


Figure 10-2 ISUP Network Interconnect - End Office to Toll Direct

If an IEC is required to complete the call and the circuit selection is an ISUP circuit directly connected to the toll office, the equal access end office switch marks the circuit busy, and formulates an IAM to send over the ISUP network to the toll office.

Following is a summary of the information provided by the various parameters of the IAM.

- **Called Party Number Parameter:** Some of the parameter subfields related to Network Interconnect provide the following information:
 - The nature of address indicator provides information about the called party number. This information is shown in Table 10-2.
 - Address information field is coded as shown in Table 10-2.

The **National Number** conforms to the North American Numbering Plan and has format NPA-NXX-XXXX. A subscriber number has the format NXX-XXXX. An international number has the format CC+NN, where CC is the country code and NN is the national number within the specified country.

Table 10-2 indicates that either 7 or 10 digits may be sent if the subscriber dialed only 7 digits. As an option, the end office is able to add the numbering plan area (NPA) digits to the address digits and send the 10 digits (NPA-NXX-XXXX). This occurs when an implied NPA appears on RC/V View 9.3.

Table 10-2 Called Party Number (CPN) and Transit Network Selection (TNS) Parameters Coding

DIALED DIGITS ^{a b}	CALLED PARTY NUMBER		TNS CIRCUIT CODE ^c
	ADDRESS FIELD ^b	NATURE OF ADDRESS	

(10XXX)+(1)+7D	7D	Subscriber Number	0ZZ
(10XXX)+(1)+7D d	NPA+7D	National Number	0ZZ
(10XXX)+1+10D	10D	National Number	0ZZ e
(1)+SAC+7D	SAC+7D	National Number	0ZZ e
(10XXX)+0+7D f	7D	Subscriber Number, Operator Requested	0ZZ
(10XXX)+0+7D e f	NPA+7D	National Number, Operator Requested	0ZZ
(10XXX)+0+10D f	10D	National Number, Operator Requested	0ZZ g
(10XXX)+011+CC+NN(#)	CC+NN	International Number	1NX
(10XXX)+01+CC+NN# f	CC+NN	International Number, Operator Requested	1NX
10XXX+0(0) f	(None)	No Number Present, Operator Requested	0ZZ g
00 d	(None)	No Number Present, Operator Requested	0ZZ e
01XXX+#	(None)	No Number Present, Cut-Through Call to Carrier	0ZZ f
950-WXXX	950-WXXX	Subscriber Number or 950+ Call from Public Station, Hotel/Motel or Non-Equal Access End Office g	0ZZ

Notes:

- a. Dialed digits are digits from:
 - A non-ISDN or stimulus mode basic rate interface subscriber
 - Digits in the Q.931 called party number information element with an optional CIC (XXX) in the TNS parameter, or network specific facilities in the information element of Q.931.
- b. The dialed digit codes are identified as follows:
 - 7D = NXX-XXXX
 - 10D = NPA-NXX-XXXX
 - SAC = Service Access Code (800, 888, 877, etc.)
 - CC = Country Code
 - NN = National Number
 - XXX = Carrier Identification Code
- c. Circuit code is a 4-bit value that is translated by RC/V View 10.23 to a 0ZZ/1NX digit string.
- d. The 5ESS[®]-2000 switch inserts the NPA on calls routed via access tandem and may add it on directly routed calls based on routing data.
- e. Use 1NX for calls routed to an international carrier (INC) and international calls routed via a consolidated carrier.
- f. The nature of address codes for "operator requested" calls apply to directly routed calls not handled by local exchange carrier operator services system.
- g. Use 1NX for calls to an INC.

- **Charge Number Parameter:** Charge information "is" or "is not" included in the IAM depending on the IEC subscription basis. The charge information consists of the equal access multifrequency II and ANI digits. The

ANI (also known as billing number) is in the charge number parameter. The II (information digits associated with the equal access call) is part of the originating line information parameter. The option for sending charge information is independent of the option for sending the CPN parameter.

The subfields of the charge number parameter are as follows:

- Nature of Address Indicator is coded to reflect if ANI digits are available.
 - Numbering plan is coded as ISDN numbering plan.
 - Address digits always includes ten digits. If all ten digits of the charge number are not available, the home NPA digits are added. The address information field is coded the same as the called party number parameter.
 - Address presentation restricted indicator is coded with the same values as the CPN parameter if either the user-provided or network provided CPN parameter is included in the IAM. If neither of the calling party number parameters are available, the indicator is coded on the basis of the privacy indicator for the customer interface as illustrated for the network-provided CPN presentation restricted indicator. If there is no privacy indicator associated with the customer interface, the address presentation restricted indicator is coded as "presentation allowed."
- **Originating Line Information Parameter (OLI):** For equal access calls the Charge parameter is included in the IAM, the Originating Line Information parameter is also included.

The OLI parameter reflects the equal access multifrequency (II) information digits relating to the characteristics of the originating line, as shown in Table 10-3 .

Table 10-3 Originating Line Information (I and II Digits)

II DIGITS	I DIGIT	MEANING	ORIGINATING LINE INFORMATION CODE
00	0 or 3	Identified Line - No Special Treatment	0
01	1 or 4	Operator Number Identification (ONI) [Multiparty]	1
02	2 or 5	ANI Failure; Unavailable	2
06	6	Hotel (Without Room Identification)	6
07	7	Coinless, Hospital, and Inmate (Screening)	7
08		Inter-LATA Restricted	8
10		Test Call	10
20		AIOD-Listed DN Sent	20
23		Coin or Non-Coin	23
24		Toll-Free Service Access Code (SAC Call, such as 800 or 888 numbers (Translated)	24
27		Coin Call	27
34		Operator Handled	34
52		OUTWATS	52
68		Inter-LATA Restricted-Hotel Line	68
78		Inter-LATA Restricted-Coinless Line	78
93		Inter-LATA Virtual Private Network Service For Example, SDN)	93
Note:			
The I and II decimal codes are administered by Bell Communications Research, Inc.			

- **Transit Network Selection (TNS) Parameter:** In calls from an end office to an IEC over direct connection to the toll office, the TNS parameter is included in the IAM only if for international calls.

The subfields of the TNS parameter are coded as follows:

- The type of network identification is coded as "national network identification."
- The network identification plan code is coded as "carrier identification code with the circuit code."
- Network identification:

The network identification is the 3-digit CIC (XXX). The customer may specify the carrier code by dialing the prefix 10XXX, or for ISDN access, the information may be specified within a Q.931 network specific facility information or TNS element. When the carrier code is not specified explicitly, the customer's prescribed CIC is used.

For toll-free Service Access Code (SAC) calls (such as 800 or 888 service calls), the carrier code is determined by analysis of the first digits. Carriers are assigned blocks of SAC+NXX numbers. Customers are not allowed to explicitly specify a carrier for service access code calls.

If equipped, the LEC may determine the carrier through a service control switching point.

- Circuit code coded by agreement between the LEC and the IEC. The code is equivalent to the 0ZZ/1NX used in EAMF signaling. It is required for international calls that circuit code 1 be used for non-operator and circuit code 2 be used for operator calls.
- **User Service Information Parameter (formerly Bearer Capability):** Voice calls and data calls for 56 kb/s, 64 kb/s (restricted) and 64 kb/s (unrestricted) are supported. Voice calls include speech and 3.1 kHz audio. The 3.1 kHz audio is treated the same as speech since no special routing is required.

For non-ISDN access, the transmission requirements are determined from the characteristics of the customer line along with any customer specified indication. One example is when the customer dials #56 to request 56 kb/s. The ISDN access transmission requirements are determined from the Q.931 bearer capability information element.

10.5.1.2 Subsequent Call Setup Message Flow

Following the IAM, a continuity check procedure is optionally done and additional messages are exchanged between the end office and the toll office. The sequence and coding of ISUP ACM and the AM that follow the IAM are usually the same as those for an intranetwork call. These are discussed in more detail in "ISDN User Part (ISUP)," Section 5.

TIAM: This timer is set waiting for an ACM, ANM, or REL. The procedures for this timer are the same as for intranetwork calls. See Table 5.5-1, ADDR COMP, for additional details on this timer.

10.5.2 ISUP End Office To ISUP Toll Office Via ISUP Access Tandem

10.5.2.1 Message Flow

Figure 10-3 illustrates the message flow between the end office and access tandem, and between the access tandem and toll office for a call setup.

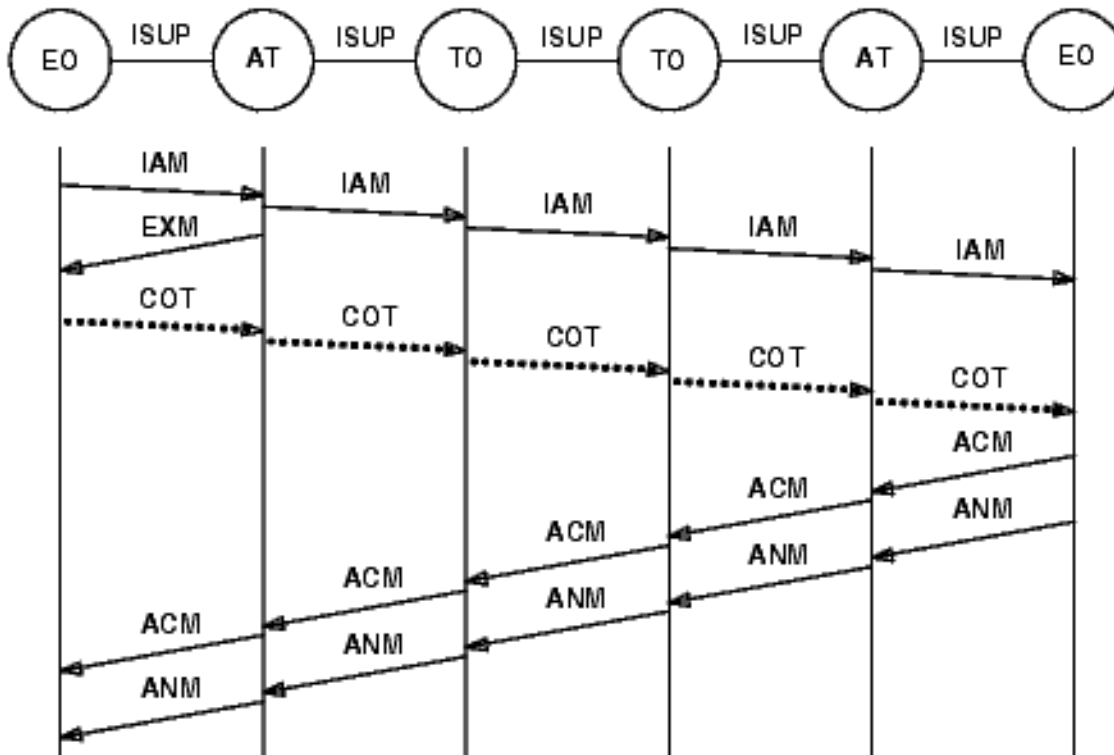


Figure 10-3 ISUP Network Interconnect Call - via Access Tandem

10.5.2.2 ISUP Equal Access End Office to ISUP Access Tandem

When the circuit selected for the call routing is to an ISUP access tandem, the end office marks the circuit busy and formulates the IAM and sends it to the access tandem office. The IAM is coded the same as for calls on direct connections to the toll office with the exception that the IAM for calls via an access tandem must include the TNS parameter.

The TNS parameter is coded as specified for the calls on direct connection to the toll office with the exception of circuit code. The circuit code to the access tandem is a binary code corresponding to the 0ZZ of the 0ZZ-XXX-digit string used in equal access multifrequency inter-LATA signaling or the 1NX of the 1NX-XXX-CCC-digit string used in EAMF INC signaling (See Table 5.5-1, CKT CODE).

There is only one timer set by the equal access end office when the IAM is sent to the access tandem.

TIAM: This timer is set waiting for an ACM, ANM, or REL. The procedures for this timer are the same as for intranetwork calls. See Table 5.5-1, ADDR COMP, for additional details on this timer.

10.5.2.3 ISUP Access Tandem to IEC Toll Office

When the IAM containing the TNS parameter is received, the access tandem selects an outgoing circuit to the toll office on the basis of the following:

- The CIC and circuit code within the TNS parameter
- The transmission medium requirement specified in the user service information parameter.

When the circuit selected is an ISUP circuit, the access tandem marks the circuit busy, formulates an IAM, and sends it to the IEC toll office.

The IAM transmitted by the access tandem contains the same parameters as the IAM received from the end office except for the TNS parameter. The access tandem determines from the TNS parameter if the IEC uses INC signaling. The TNS parameter is included in the outgoing IAM to the toll office if INC signaling is used.

After sending the IAM to the toll office, the access tandem switch sets two timers.

TIAM: This timer is set waiting for an ACM, ANM, or REL. The procedures for this timer are the same as for intranetwork calls. See Table 5.5-1, ADDR COMP, for additional details on this timer.

TEXM.D: This timer is set to provide a delay to reasonably ensure that glare and blocking are not encountered on the outgoing circuit. See Table 5.5-1, EX MD TIMER, for more details.

If glare is encountered and the access tandem controls the circuit, the access tandem switch proceeds with call setup and the timer is unaffected. However, if an event occurs which causes the access tandem to make an automatic repeat attempt, another circuit must be selected. Some of the events that could cause automatic repeat attempt are as follows:

- Access tandem does not control the circuit
- Outgoing continuity check failed.

When the **TEXM.D** timer expires, the access tandem formulates the exit message (EXM) and sends it back to the ISUP end office. The exit message contains the binary coded digital representation of the trunk group number used between the access tandem and the toll office.

The access tandem must send the EXM before any of the following:

- Sending to the end office an ACM, ANM, or a REL received from the toll office.
- Sending to the end office any REL generated by a reattempt failure for the call on the circuit group to the toll office.

10.5.2.4 Incoming Continuity Check

If a continuity message received by the access tandem from the end office indicates that a continuity check has failed, the access tandem sends a REL for the outgoing circuit to the toll office. The REL contains the cause coded for a "temporary failure" and the location shown "local network." The access tandem omits sending the EXM and cancels the **TEXM.D** timer.

Following the transmission of the IAM, the continuity check and subsequent message exchange between the access tandem and end office are the same as intranetwork calls.

10.5.2.5 Access Tandem/Service Switching Point to Toll Office

10.5.2.5.1 Identifying SSP Calls

An access tandem that is equipped with the SSP feature determines if a call requires SSP procedures by examining the CIC (encoded as a pseudo-carrier) in the TNS parameter of the IAM. The SSP calls can also be recognized by a trigger of NS800 associated with translation of the IAM's circuit code (RC/V Views 10.23, 9.30, 9.35, and 9.5). If the TNS parameter is not in the IAM, the call requiring SSP processing is recognized by the address digits in the called

party number parameter. The number format is either SAC-NXX-XXXX or 00Y-NXX-XXXX.

10.5.2.5.2 Processing the Call by the Access Tandem

The access tandem switch uses the information provided in the IAM to query the service control point (SCP) data base to obtain routing instructions. If the call requires routing to an IEC, the SCP data base provides a IEC CIC and a called number. The access tandem selects an outgoing trunk circuit based on the carrier code and other routing information provided by the SCP data base. If ISUP signaling is used on the outgoing circuit, the access tandem marks the circuit busy and forms and transmits the IAM for the outgoing circuit. The IAM is coded in the same way as the IAM from the end office with the following exceptions:

- The called number returned by the SCP data base is coded into the called party number parameter.
- If the SSP 800 feature is being provided and the number returned by the SCP data base does not have a toll-free SAC prefix (such as 800 or 888), the originating line information parameter is coded with the binary equivalent of the decimal value 24; otherwise, the OLI parameter is used.
- If the IEC subscribes to charge information and none was included in the received IAM, the outgoing IAM includes a charge number parameter coded as follows:
 - Odd/Even indicator is coded "ODD" (1).
 - Nature of address indicator is coded "automatic number identification of the calling party; national number."
 - The numbering plan is coded for the "ISDN numbering plan."
 - The address digits are coded with the appropriate NPA digits.
 - The address presentation restricted indicator is coded for "presentation allowed."
- The originating line information parameter is coded to a binary equivalent value of the decimal 23 unless previously coded with the value of 24.

The procedures for incoming continuity check and subsequent call setup are the same as covered previously.

10.5.3 Equal Access Inband Signaling To ISUP Signaling

10.5.3.1 Overview

This section contains procedures that are involved at an ISUP access tandem for interworking equal access inband signaling to ISUP.

10.5.3.2 Equal Access End Office to Access Tandem - Inband Signaling

Figure 10-4 illustrates the interworking between the exchange access inband signaling and ISUP signaling for a call between the LEC end office and an inter-LATA toll office. Figure 10-5 illustrates the interworking between the inband signaling and ISUP signaling between the LEC and an international toll office.

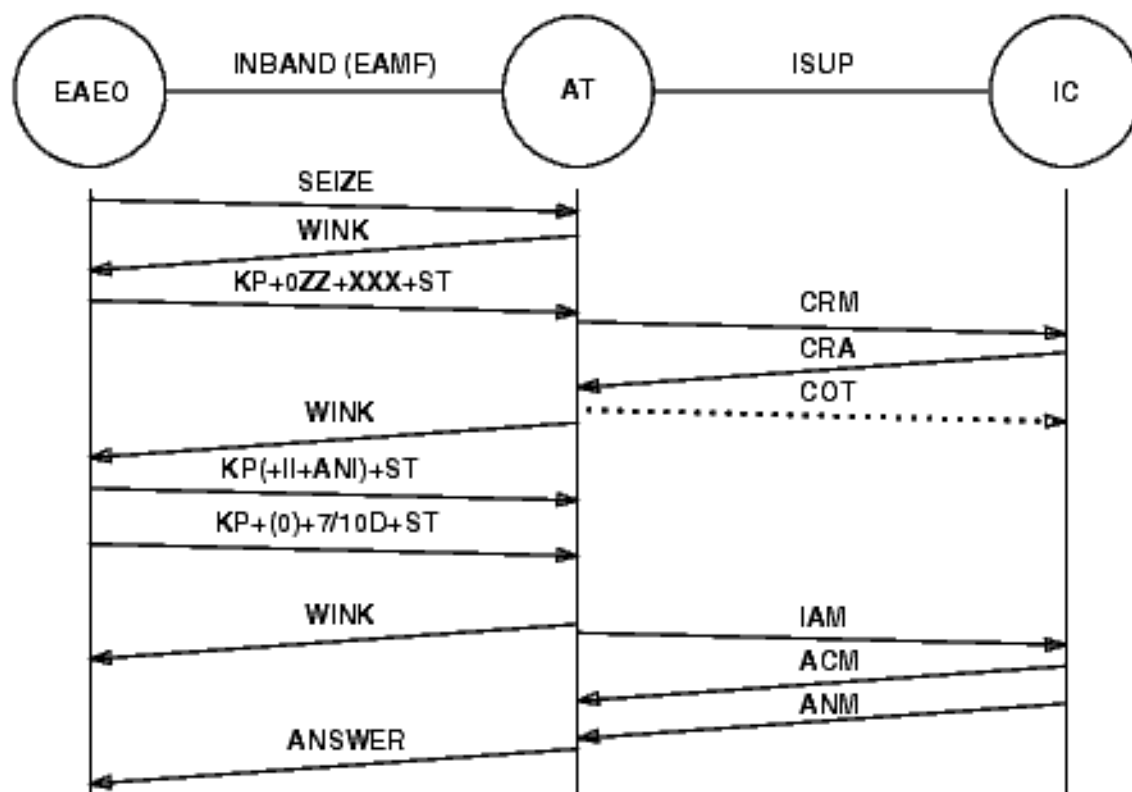


Figure 10-4 Interworking - Equal Access End Office to Inter-LATA Carrier

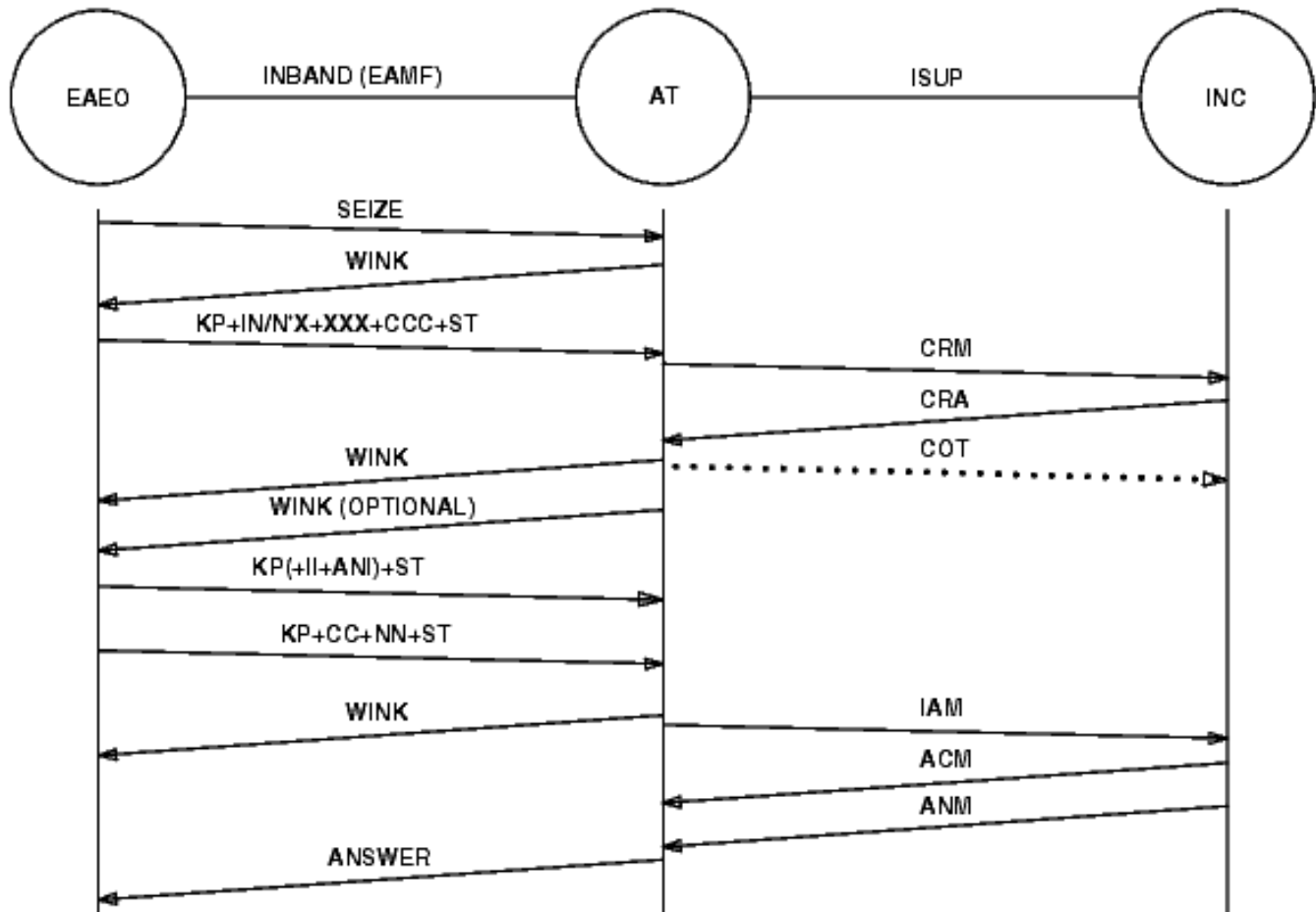


Figure 10-5 Interworking - Equal Access End Office to International Carrier

10.5.3.3 ISUP Access Tandem Procedures

Following are the procedures used at an ISUP access tandem for setting up a connection for a call requiring equal access inband and ISUP interworking.

(1) **Circuit Reservation Procedure:**

If the outgoing circuit to the IEC uses ISUP signaling, the access tandem marks the circuit busy and prepares the Circuit Reservation Message (CRM) for the outgoing circuit.

The CRM contains the nature of connection indicator parameter coded the same as for an IAM. If a continuity check is required on the outgoing circuit, it is requested in the CRM. The transmission path is not completed when the CRM is sent.

After sending the CRM, the access tandem sets the **TCRM** timer to wait for the Circuit Reservation Acknowledgement (CRA) message (See Table 5.5-1, CRA TIMER, for more details) from the IEC. The access tandem must be prepared to receive a release from the IEC or an on-hook disconnect signal from the equal access end office. Upon receipt of any of these, the access tandem cancels the **TCRM** timer.

If the **TCRM** timer expires before receiving any of the previous mentioned messages or signal, the access tandem sends a Rel to the toll office for the outgoing circuit. The

parameters in the Release message are coded as follows:

- Location is coded "local local network"
- Cause value is coded "temporary failure."

Assuming another ISUP trunk is selected, the access tandem will retry the call by selecting a second outgoing circuit. A circuit reservation message is sent for the new circuit to the IEC. The **TCRM** timer is set again. If the timer **Tcrm** expires again, the access tandem sends a tone or recorded message back to the end office and then sends a disconnect signal (on-hook) back to the end office.

A continuity check (if needed) can begin after sending the CRM. The access tandem waits for the continuity check to complete before sending a continuity message to the IEC indicating whether the continuity check succeeded or failed. If the continuity check fails, the access tandem selects another outgoing circuit.

NOTE: Receipt of a CRA and the completion of the continuity check are independent of each other and either may occur first.

(2) **Second Inband Sequence:**

After the circuit reservation acknowledgement has been received and the continuity check on the outgoing circuit is successfully completed, the access tandem returns a wink to the end office to trigger the second stage of outpulsing.

For transitional INC signaling, an optional second wink may be sent to represent the wink that would be regenerated from the IEC if the outgoing trunk used inband signaling. There must be at least a 200-ms delay before the access tandem returns the second wink.

After returning the winks, the access tandem receives the second stage inband sequence from the end office as shown in Table 10-4 for inter-LATA signaling and Table 10-5 for international signaling.

Table 10-4 Inter-LATA Signaling

FIRST INBAND SEQUENCE	SECOND INBAND SEQUENCE	ADDRESS FIELD	NATURE OF ADDRESS INDICATOR
KP+0ZZ+XXX+ST	KP+(II+ANI)+ST KP+7D+ST	7D	Subscriber Number
KP+0ZZ+XXX+ST	KP+(II+ANI)+ST, KP+10D+ST	10D	National (Significant) Number
KP+0ZZ+XXX+ST	KP+(II+ANI)+ST, KP+0+7D+ST	7D	Subscriber Number, Operator Requested
KP+0ZZ+XXX+ST	KP+(II+ANI)+ST, KP+0+10D+ST	10D	National Number, Operator Requested
KP+0ZZ+XXX+ST	KP+(II+ANI)+ST'	(None)	No Number Present, Cut-Through Call to Carrier
KP+0ZZ+XXX+ST	KP+(II+ANI)+ST, KP+0+ST	(None)	No Number Present, Operator Requested
KP+0ZZ+XXX+ST	KP+(II+ANI)+ST,"	950-WXXX ^a	950+Call From Public Station, Hotel/Motel Line or Non-EAEO
KP+0ZZ+XXX+ST	KP+(II+ANI)+ST'''	950-WXXX ^a	Subscriber Number ^b
Notes: a. Use XXX from EAMF First Inband Sequence.			

b. 950+ call not from a public station or hotel/motel line.

Table 10-5 International Carrier Signaling

FIRST INBAND SEQUENCE	SECOND INBAND SEQUENCE	ADDRESS FIELD	NATURE OF ADDRESS INDICATOR
KP+1NX+XXX+CCC+ST	KP+(II+ANI)+ST, KP+CC+NN+ST	CC+NN	International Number
KP+1N'X+XXX+CCC+ST	KP+(II+ANI)+ST, KP+CC+NN+ST	CC+NN	International Number, Operator Requested
KP+1NX+XXX+01R+ST	KP+(II+ANI)+ST, KP+10D+ST	10D	National (Significant) Number
KP+1N'X+XXX+01R+ST	KP+(II+ANI)+ST, KP+10D+ST	10D	National Number, Operator Requested
KP+1NX+XXX+000+ST	KP+(II+ANI)+ST'	(None)	No Number Present, Cut-Through Call to Carrier
KP+1N'X+XXX+000+ST	KP+(II+ANI)+ST, KP+0+ST	(None)	No Number Present, Operator Requested

(3) **Acknowledgement Wink:**

The access tandem returns an acknowledgement wink to the equal access end office after receiving the second stage inband sequence. The acknowledgement wink appears to the end office as if it were sent from the IEC and passed by the access tandem. There must be a delay of at least 200 ms before returning the acknowledgement wink.

(4) **Initial Address Message (IAM):**

After the acknowledgement wink has been returned, the access tandem generates and sends an IAM to the IEC. The IAM is coded the same as discussed for all ISUP connections with the following exceptions:

- **Nature of Connection Indicator:** The continuity check indicator is coded "continuity check not required" since any required check is requested as part of the circuit reservation message.
- **Forward Call Indicators Parameter:** This parameter is coded to include the following:
 - Not an incoming international call
 - No end-to-end method available
 - Interworking encountered
 - No end-to-end information available
 - ISDN user part not used all the way
 - ISDN user part not required all the way
 - Originating non-ISDN access.
- **Calling Party's Category Parameter:** This parameter is coded "calling party category unknown."
- **Called Party Number Parameter:** This parameter is coded as follows:

- Odd/Even Indicator: Depending on the number of digits (odd or even) in the address digits as shown in Tables 10-4 and 10-5 .
 - Nature of Address Indicator: Coded to correspond with the received inband sequence as shown in Tables 10-4 or 10-5 .
 - Numbering Plan Code is "ISDN Numbering Plan."
 - Address Digits: The address digits are shown in Tables 10-4 and 10-5 . The address digits 950-0XXX are derived from the CIC (XXX) received in the first inband sequence. When no address digits are to be sent, the address digit bytes are omitted. For INC signaling, the address digits include the country code digits in the case of the first two sequence in Table 10-5 . When the country code digits are included, they are not padded to three digits as is done in the first inband sequence.
- **User Service Information Parameter:** This parameter is coded to agree with the incoming trunk type. On inband signaling trunks, voice and 56 kb/s digital data calls are supported. Therefore, this parameter is coded as specified for voice call - speech or digital data call - 56 kb/s, as appropriate.
 - **Transit Network Selection Parameter:** This parameter is only included in the IAM for INC signaling. The coding is the same as specified for all ISUP signaling calls.
 - **Charge Information:** If the II + ANI digits have been received, the IAM message must contain the originating line information parameter and the charge number parameter.
 - Originating line information parameter is coded with the binary equivalent of the II digits received as shown in Table 10-3 .
 - Charge number parameter is coded with the received ANI digits.

The address presentation indicator is coded according to the ANI privacy indicator for the incoming trunk. In the event that there is no ANI private indicator associated with the incoming trunk group, the address presentation restriction indicator is coded with the default value "presentation allowed."
 - The IAM does not include a CPN, access transport, or *user-to-user information* parameter.

(5) **Timers:** After sending the IAM, the access tandem sets **TIAM** timers as discussed earlier.

(6) **Subsequent Call Setup:** Upon receipt of the address complete message or the answer message, the access tandem completes the transmission path. If an answer message is received, the access tandem immediately sends answer supervision to the incoming circuit.

10.5.3.4 Traditional Inband Signaling to ISUP Signaling

Described here are the procedures at an ISUP access tandem for interworking traditional inband signaling from an end office to ISUP on the outgoing circuit to an inter-LATA or international toll office. Figures 10-6 and 10-7 illustrate this interworking.

- ***Direct Distance Dialing - Single Stage Outpulsing:***

When the ISUP access tandem receives the inband sequence KP+7/10D+ST on the incoming circuit from the end office, it performs code interpretation and circuit selection to determine if interworking with ISUP applies.

If the outgoing circuit to the IEC uses ISUP signaling, the procedures for intranetwork calls given in Section 5, are used with the following exceptions:

- If the incoming circuit is a centralized automatic message accounting (CAMA) circuit, the ISUP access tandem returns an off-hook on the incoming circuit to obtain a single information digit and the ANI. For other types of circuits, the ANI is not available. When the ANI is obtained, the IAM will not contain an originating line information or charge number parameter.
- The coding for the user service information parameter for 56 kb/s digital data calls is the same as covered previously in the ISUP call setup arrangement.

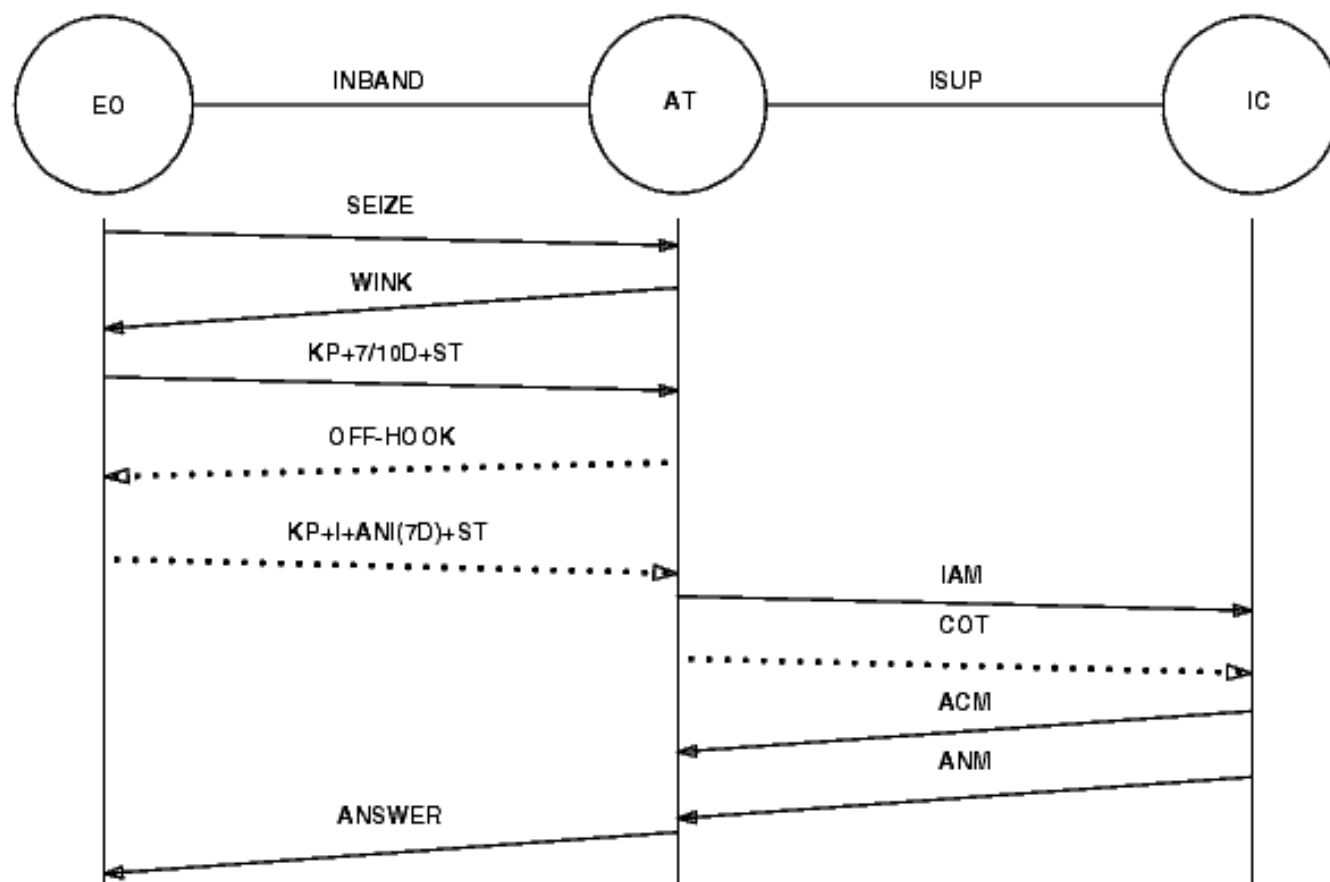
- ***International Direct Distance Dialing - Two-Stage Outpulsing:***

When the access tandem receives the inband sequence KP+011+PCC+ST on the incoming circuit from the end office, it performs code interpretation and circuit selection to determine if interworking with ISUP is required. This type of call is always routed to the carrier that supports international direct distance dialing under traditional signaling.

NOTE: Calls that are handled by a local operator system must be routed on inband signaling trunks and cannot be interworked with ISUP signaling.

If the outgoing trunk to the IEC uses ISUP signaling, the access tandem proceeds in the same manner as for equal access inband signaling with the following exceptions.

- After returning the wink to the end office, the second inband sequence received is KP+CC+NN+ST.
- The access tandem does not return an acknowledgement wink to the end office.
- The subsequent IAM sent to the IEC *must not* contain a charge number or originating line information parameter since the ANI is not provided for traditional inband signaling.
- The TNS parameter in the IAM contains the IEC CIC code and the circuit code.



NOTE: OFF-HOOK REQUESTS FOR ANI APPLIES ONLY TO CAMA TRUNKS.

Figure 10-6 Interworking - Traditional Inband Signaling End Office to Inter-LATA Carrier

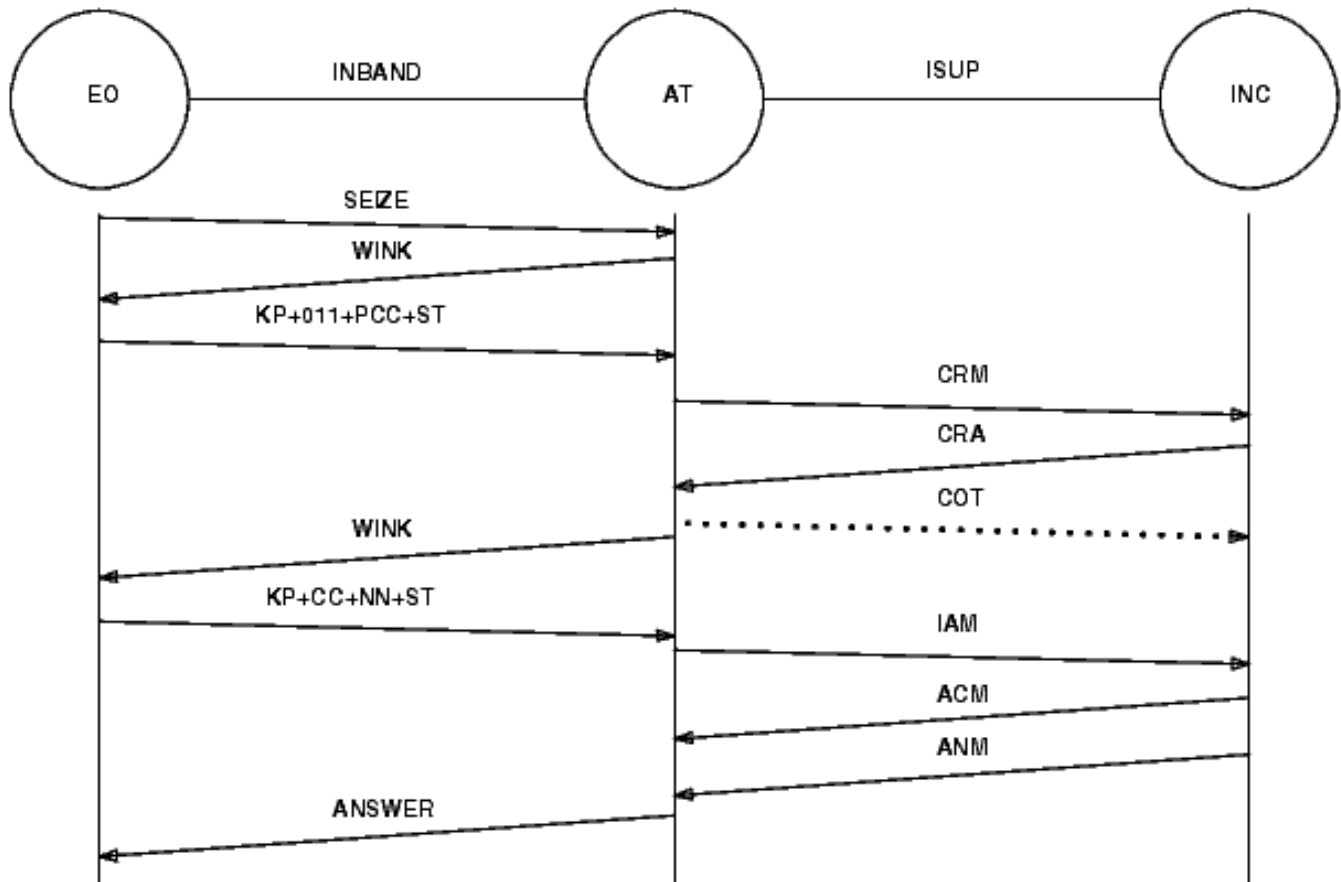


Figure 10-7 Interworking - Traditional Inband Signaling End Office to International Carrier

10.5.3.5 Signaling Interworking with Service Switching Point Feature - Procedural Description

This part describes the procedures at the ISUP access tandem when the incoming circuit from an end office uses inband signaling and the access tandem provides the service switching point feature and routes the call to an ISUP outgoing trunk to the inter-LATA or international toll office. The incoming call may be received from the end office using equal access, CAMA, or traditional inband signaling. The procedures for each of these types of inband signaling are discussed in the following text:

- (1) **Equal Access Inband Signaling:** Under service switching point procedures, the access tandem (service switching point) determines from the CIC that the service requires switching service point processing. The CIC contains the number service code rather than the IEC code. The SSP calls can also be recognized by a trigger of NS800 associated with translation of the impulsed 0ZZ code (RC/V Views 9.30 and 9.5).

Following are the procedures followed by the access tandem for number service calls from equal access end offices:

The access tandem queries the SCP data base for routing based on the received information. The SCP data base returns an inter-LATA or international CIC and a call number for calls requiring this type of routing. The access tandem selects the outgoing circuit based on the information received from the SCP data base. If the outgoing circuit uses ISUP signaling, the access tandem marks the circuit busy and generates an IAM for the outgoing circuit. The IAM is coded as specified for other equal access inband signaling calls with the following exceptions:

- The continuity check indicator in the nature of connection indicators parameter is coded to indicate if a continuity check is required on the outgoing circuit.
- The called number returned from the SCP data base is coded in the called party parameter.
- If the SSP 800 feature is being provided and the called number returned by the SCP does not start with a toll-free Service Access Code (SAC), such as 800 or 888, the originating line information parameter is coded with the binary equivalent of the decimal value 24; otherwise, the received II (information) digits are used.
- If the IEC subscribes to charge information and none was received, the IAM includes a charge information coded as follows:
 - Odd/Even indicator coded "odd."
 - Nature of address indicator coded "Automatic number identification of the called party; natural number" if number plan area (NPA) digits are provided; otherwise "automatic number identification not provided." For the coding "automatic number identification not provided, the byte 1 is the last byte included.
 - Numbering plan is coded "ISDN numbering plan."
 - Address digits are coded with the appropriate NPA digits, if possible; otherwise, no address digits are included.
 - Address presentation restricted indicator is coded "presentation allowed."
- The originating line information parameter is included and unless coded with value 24, it is coded with the binary equivalent of the decimal value 23.

(2) **CAMA Signaling:**

The access tandem recognizes that the call requires SSP-800 processing by examining the called number (either SAC-NXX-XXXX or 00Y-NXX-XXXX).

The access tandem procedure for selecting routing is the same as for equal access inband signaling.

The IAM is coded the same as for calls using ISUP signaling from the end office with the following exceptions:

- The I (information digit) is received rather than the II digits. These are treated the same as the II. Table 10-3 shows the relationship between I and II information digits.
- If a seven-digit ANI is received, the access tandem adds the NPA digits as a prefix to the seven digits and code. The nature of address indicator in the change number parameter is coded "automatic number identification of the calling party; national number." If this is not possible, the nature of address indicator is coded "ANI of the calling party; subscriber number."
- If no ANI digits are received and the IEC subscribes to charge information, the appropriate NPA is provided as it is for equal access signaling.

(3) **Traditional Inband Signaling:**

The SSP procedures at the ISUP access tandem are essentially the same as for equal access signaling with one exception to the IAM. The exception is that since traditional inband signaling does not provide the ANI, if the IEC subscribes to charge information, the appropriate NPA is provided.

10.5.4 ISUP Signaling To Equal Access Inband Signaling

10.5.4.1 Local Exchange Carrier to Inter-LATA or International Carrier

This part describes the procedures at an access tandem for handling calls from an ISUP end office destined for an IEC over outgoing trunks using equal access inband signaling. Figures 10-8 and 10-9 illustrate the interworking process.

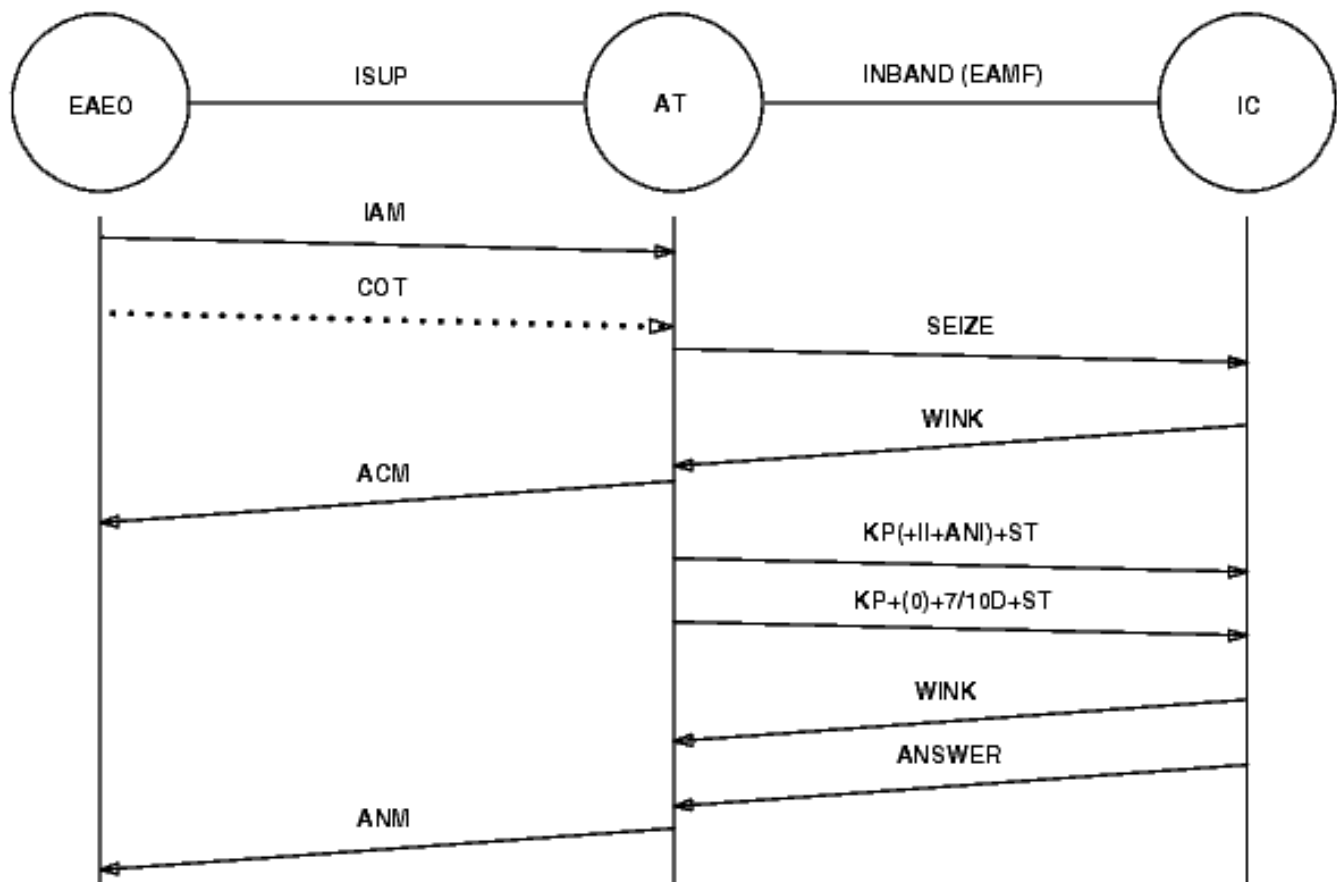


Figure 10-8 Interworking ISUP to Equal Access Inband Signaling - Inter-LATA Carrier

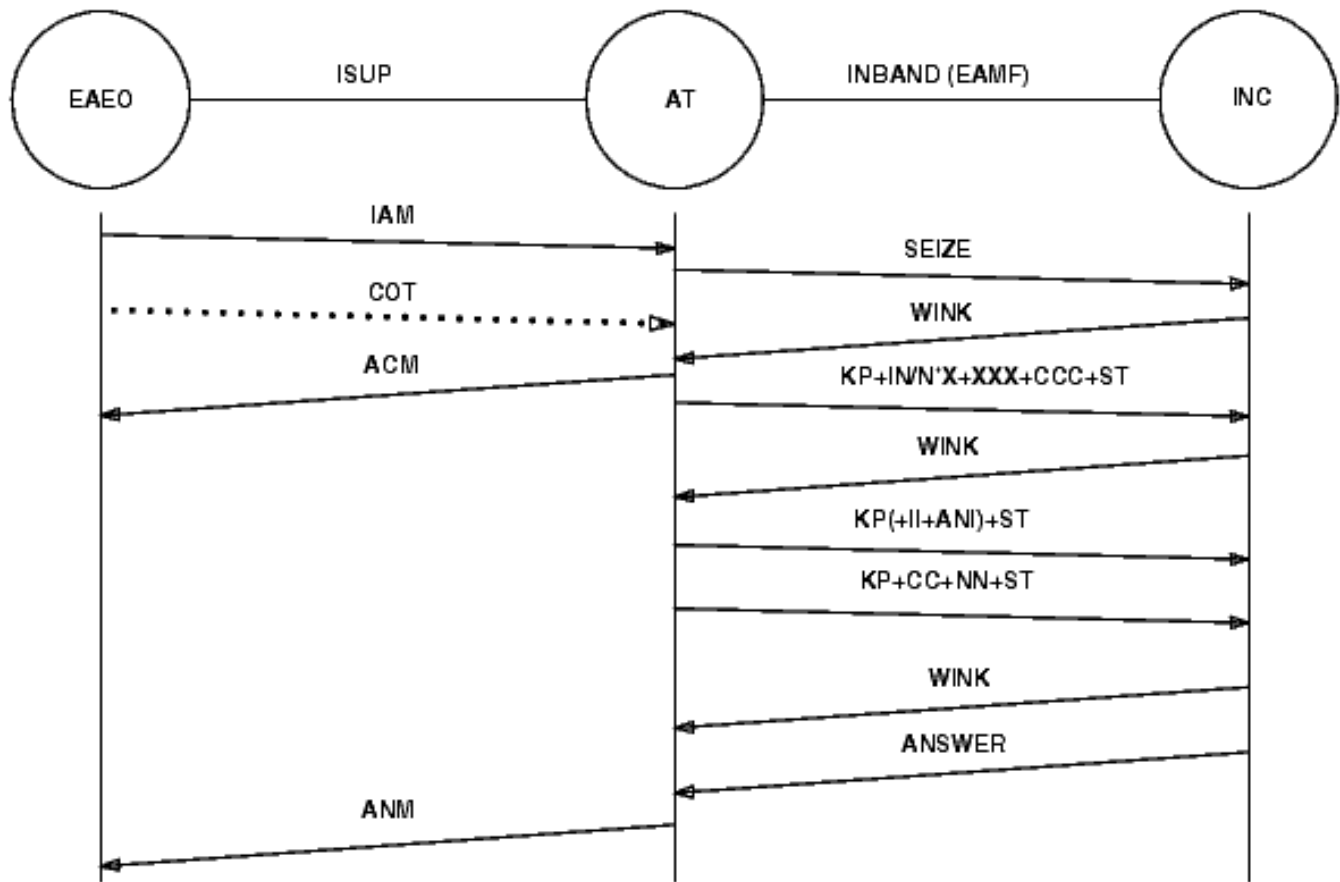


Figure 10-9 Interworking ISUP to Equal Access Inband Signaling - International Carrier

When the access tandem receives an IAM containing a TNS parameter, the access tandem selects an outgoing circuit and determines the need for equal access inband signaling from the following:

- Carrier code and circuit code in TNS parameter
- Transmission medium requirements specified in the user service information parameter.

The following summarizes the interworking procedures:

(1) **Outgoing Circuit Seizure:**

At an access tandem (AT), seizure of an outgoing equal access multifrequency (EAMF) signaling circuit is delayed if a continuity test is being performed on the incoming circuit to wait for the receipt of a COT message from the equal access end office (EAO). When the AT receives either a REL or a COT message from the EAO, it cancels the **TCRR.R** timer.

The procedures for expiring timers are covered later in this section. These procedures are applicable if the timer expires before an appropriate message is received.

The procedures for handling the continuity check message with a "continuity check failed" indication are discussed later in this section.

When the continuity message contains a "continuity check was successful" or if no continuity check is being performed, the access tandem seizes the outgoing circuit to the IEC and waits

for the return wink.

(2) **Address Complete Message:**

When the access tandem receives the return wink from the IEC, it generates and sends an address complete message for the incoming circuit to the ISUP end office.

The backward call indicators parameter in the address complete message are coded to indicate the following:

- No charge indication
- No called party status indication
- No end-to-end method available
- Interworking encountered
- No end-to-end information available
- ISDN user part not used all the way
- Holding not required
- Non-ISDN access.

(3) **Inband Sequence Outpulsing:**

After the return wink is received from the IEC, the access tandem determines from the circuit code in the TNS parameter whether IEC signaling is required on the outgoing circuit. The access tandem then outpulses the appropriate inband sequence to the IEC.

The outpulse sequence depends on the nature of address indicator and the address digits in the received called party number parameter. The relationship among the nature of address indicator, address digits, and the inband sequence is shown in Table 10-4 for inter-LATA signaling, and Table 10-5 for international signaling. The access tandem outpulses only the second stage sequence for inter-LATA signaling. Both the first and second stage sequences are outpulsed for international signaling. When outpulsing for international signaling, the access tandem waits for a return wink from the IEC after outpulsing the first stage before outpulsing the second stage.

If the nature of address indicator contains a value not supported in Table 10-4 or Table 10-5, the call is released and a release message is returned. The cause value is coded "invalid parameter contents" and the location value is coded "local interface controlled by this signaling link."

When INC signaling is used, the access tandem determines the 3-digit country code to be outpulsed in the first inband sequence from the address digits in the called party number parameter. The form of the country code is determined from the nature of address indicator in the called party number parameter. For service access code calls to a carrier outside the continental United States, the destination digit is "0" indicating "no destination information available."

NATURE OF ADDRESS	ADDRESS DIGITS	THREE-DIGIT CODE

INDICATOR		
International Number	CC+NN	CCC (Padded CC)
National Number	NPA+7D	01R (Based on NPA)
No Number Present	None	000

If the originating line information parameter is included in the received IAM, the II (information digits) plus the ANI are sent. The II (information digits) are determined from the originating line information parameter and the mapping shown in Table 10-3. The ANI is determined as follows:

- If the IAM contains the charge number parameter containing 3 or 10 digits, these digits are the ANI.
- If the nature of address indicator in the called number parameter is coded "ANI not available," no ANI is sent (KP + ST).
- When the CPN parameter is included in the IAM and the charge number parameter is not included, the CPN is taken as the ANI. If the CPN consists of only 6 digits, the first 3 are considered the ANI.
- If neither the charge number or CPN parameters are included, no II (information digits) or ANI digits are sent (KP + ST).

After the appropriate inband sequence has been outpulsed to the IEC, the access tandem waits for an acknowledgement wink to be returned. The access tandem has the transmission path complete by the time the acknowledgement wink is received.

(4) **Subsequent Call Setup:**

If an off-hook answer signal is received on the outgoing circuit after the wink acknowledgement, the access tandem creates and sends an answer message for the incoming circuit to the ISUP end office.

10.5.4.2 Call Setup ISUP Signaling to Traditional Inband Signaling

Discussed here are the interworking procedures at an access tandem where the circuit from the end office uses ISUP signaling and the outgoing circuit to the IEC uses traditional inband signaling. Figure 10-10 illustrates the interworking between the ISUP signaling messages and the traditional inband signaling functions.

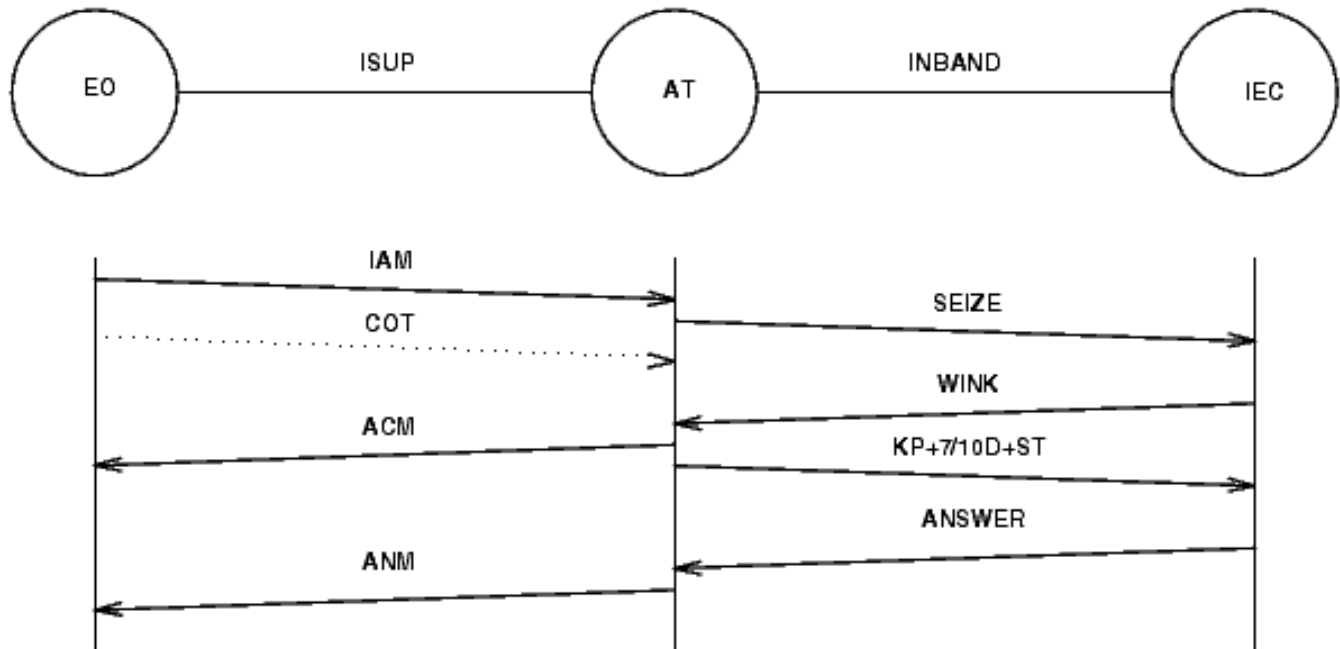


Figure 10-10 Interworking ISUP Signaling to Traditional Inband

When the IAM from the end office containing a TNS parameter is received, the access tandem determines that interworking with traditional inband signaling is required by:

- Code interpretation of the carrier code and circuit code in the TNS parameter
- Checking transmission medium requirements specified in the user service information parameter.

The interworking procedures used by the access tandem are in accordance with those shown in "ISDN User Part (ISUP)," Section 5.

10.5.4.3 Interworking at an Access Tandem - Service Switching Point

Discussed here is the interworking procedure at an access tandem that provides the Service Switching Point feature for calls from an ISUP end office routed to an IEC over outgoing inband signaling circuits.

The access tandem recognizes that the call requires service switching point processing by matching the CIC to the number service (pseudo) carrier or by recognizing the trigger of NS800 associated with translation of the IAM's circuit code (RC/V Views 10.23, 9.30, and 9.5). This information is contained in the TNS parameter. However, if the TNS parameter is not included in the IAM, the access tandem recognizes that the call requires SSP 800 processing if the address digits in the called party number parameter are in the form SAC-NXX-XXXX or 00Y-NXX-XXXX.

The access tandem uses information from the IAM to query the SCP data base for routing instructions. On the basis of the CIC and other information provided by the SCP data base, the access tandem selects an outgoing circuit. If the outgoing circuit uses exchange access inband signaling or traditional inband signaling, the procedures covered earlier are applicable. For either type of inband signaling, the called party number returned by the SCP is used as the address digits. For equal access inband signaling, the following also applies:

- If the SSP 800 feature is being provided and the SCP returns a called number that does not start with a toll-free Service Access Code (SAC), such as 800 or 888, the decimal value 24 is used for the II (information) digits; otherwise, the decimal equivalent of the code in the originating line information parameter is used as the II information digits.

- If the IEC subscribes to charge information and none is provided in the received IAM, the access tandem sends the appropriate NPA digits as the ANI along with the II information digits of 23. If the NPA digits cannot be provided, no II or ANI digits are sent. The ANI field consists of KP + ST.

10.5.5 Feature Group B - 950+ Calls

10.5.5.1 FGB Call Identification

Feature Group B (FGB) calls are identified by the dialed digits which have a 950+prefix. Carriers that choose to receive Feature Group B calls are designated as equal access plan or Feature Group B carriers.

Feature Group B was originally conceived as means to provide access from an end office to an IC carrier before deployment of full equal access signaling (Feature Group D). To make a Feature Group B call, a subscriber dials 950-WXXX and is cut through to the carrier for further call processing.

The initial deployment of Feature Group B was called the "interim plan" because it was expected that FGB would be replaced by Feature Group D access when Feature Group D became available. Signaling used for the "interim" type calls resembles traditional signaling protocol.

Under a transition plan from Feature Group B to Feature Group D, subscribers could dial either 950-WXXX or use normal equal access dialing (either 1+10D or 10XXX+10D). Signaling used for "transition" type calls resembles normal equal access signaling protocol. Both the "interim plan" and "transition plan" signaling have been extended for support by ISUP network interconnect.

Access arrangements for the "interim" plan 950-WXXX dialed calls are illustrated in Figure 10-11. Traditional Feature Group B signaling protocol (Recent Change View 10.2 SIG PRO=Feature Group B) is used. The calls, if directly routed to the Feature Group B carrier, must be on an multifrequency trunk. The calls can be routed through an access tandem switch where interworking between multifrequency and ISUP signaling may occur.

With ISUP network interconnect, 950+ calls to an equal access plan carrier via equal access signaling can be routed directly to the IC or via an access tandem using ISUP signaling. Interworking between the equal access multifrequency signaling and ISUP is supported at the end office and access tandem. Access arrangements for the "transition" plan 950-WXXX dialed calls are illustrated in Figure 10-12. Equal access signaling protocol (Recent Change View 10.2 SIG PRO=Equal Access) is used and the calls can go directly to the Feature Group B carrier or be routed through an access tandem switch; interworking between equal access multifrequency and equal access/ISUP signaling may occur at the access tandem switch, but it is not critical as with "interim" plan FGB calls.

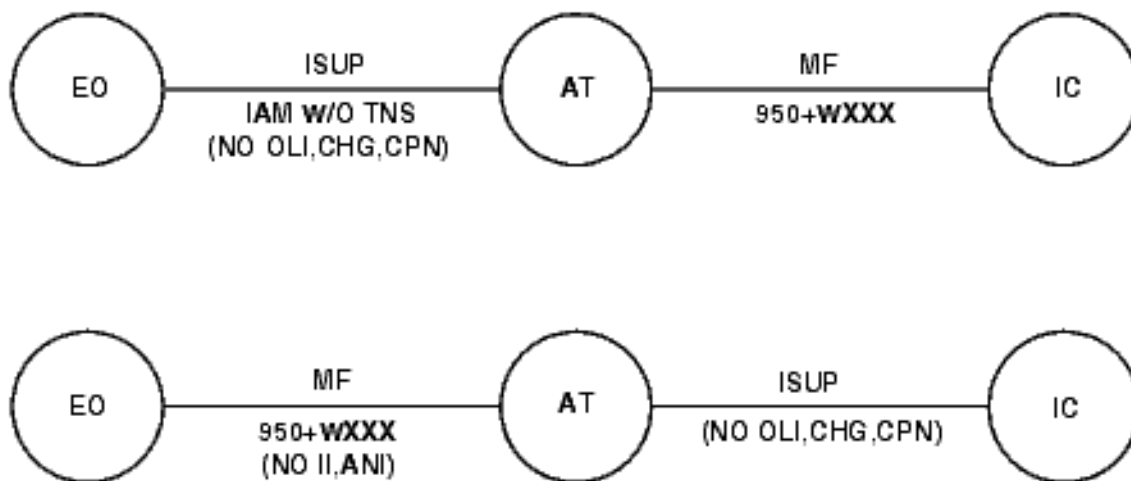
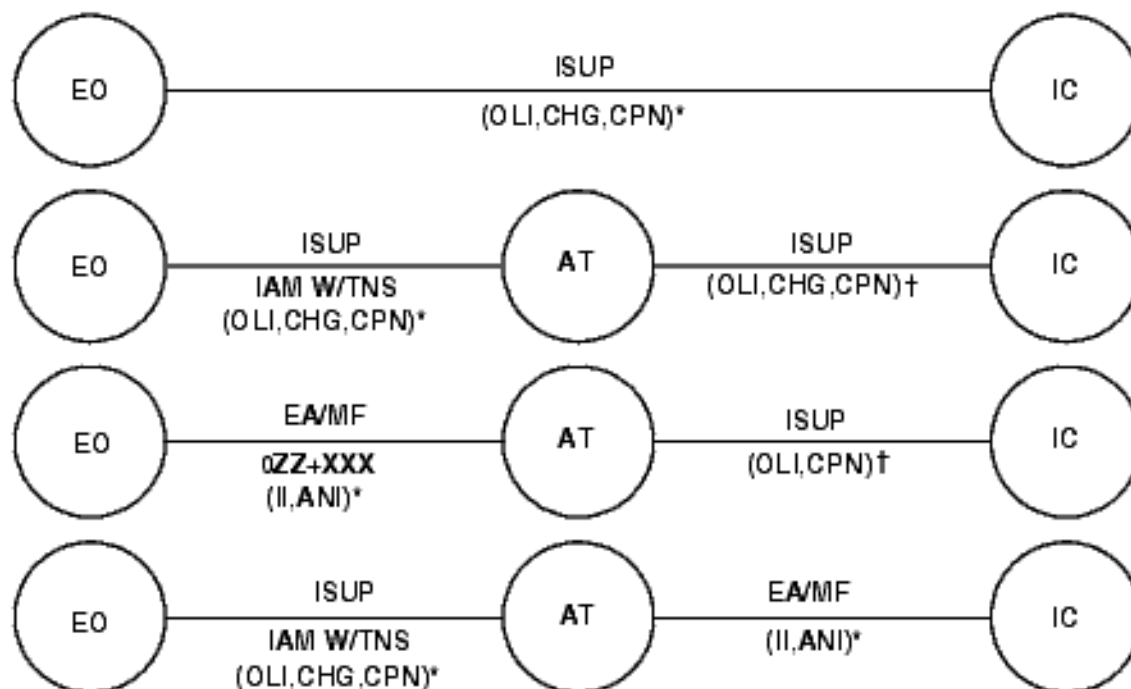


Figure 10-11 950 + Call to Feature Group B Carrier via Traditional Signaling



* - BASED ON IC SUBSCRIPTION OPTIONS

† - BASED ON INFORMATION RECEIVED FROM EO

Figure 10-12 950 + Call to Equal Access Plan Carrier via Equal Access Signaling

The distinctions between "equal access" and "traditional" signaling is illustrated as follows:

Signaling Type	TNS in IAM from EO to AT	Called Party Number Nature of Address	Charge Information & Calling Party Number
equal access	yes	subscriber number or 950+ call	provided based on IC subscription
traditional	no	subscriber number	not provided

10.5.5.2 Call Setup - Feature Group B Inband Signaling to ISUP Signaling

This is a description of the procedures at the ISUP access tandem when interworking Feature Group B inband signaling from a *non-conforming end office* trunk to an ISUP signaling trunk to an IEC. Figure 10-13 illustrates this interworking.

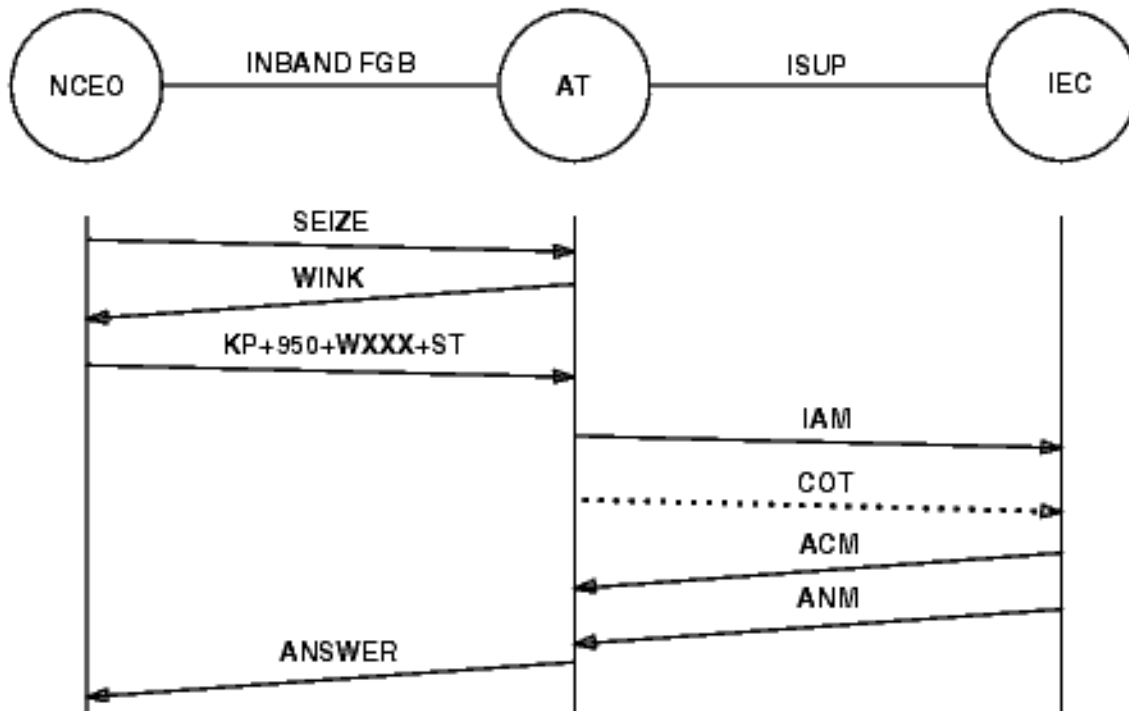


Figure 10-13 Interworking - FGB Inband NC End Office to Inter-LATA or International Carrier

The following are the procedures used at the ISUP access tandem switch:

- When the access tandem receives the inband address digits for the Feature Group B call, 950-WXXX (50-WXXX or 0-WXXX from step-by-step offices) from a non-conforming end office, it performs circuit selection based on the WXXX digits to determine if interworking with ISUP applies.
- If the outgoing circuit to the IEC uses ISUP signaling, the access tandem marks the circuit busy and generates and sends an IAM for the outgoing circuit to the IEC.
- In the IAM, the called party number parameter is coded "network specific: 950+ call from public station or hotel/motel line or equal access end office" and the numbering plan is coded for ISDN numbering plan and contains the address digits 950-WXXX. If the received digits are 50-WXXX, the access tandem adds a prefix of 9. If the received digits are 0-WXXX, the access tandem adds a prefix of 95.
- The IAM does not contain the charge number, originating line information, or CPN parameter.

10.5.5.3 Call Setup for ISUP Signaling to Feature Group B Inband Signaling

A summary of Feature Group B access arrangements supported by the ISUP network interface is provided earlier under the heading "FEATURE GROUP B - 950 CALLS."

Figure 10-14 illustrates the interworking for a Feature Group B call incoming to an access tandem from an end office using ISUP signaling and outgoing to an IEC using inband Feature Group B signaling.

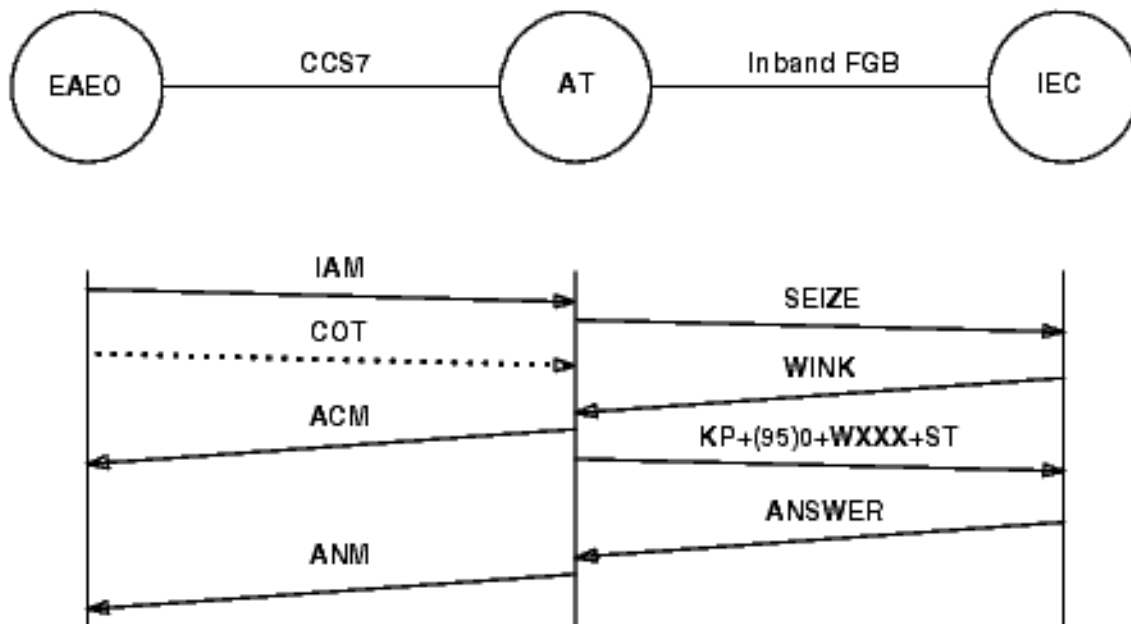


Figure 10-14 ISUP Signaling to Feature Group B Inband Signaling

The following are some of the interworking procedures used at the access tandem:

- If the received IAM contains a TNS, the interworking procedures used for ISUP to equal access inband signaling apply.
- If the received IAM does not contain a TNS parameter but has a called party number parameter containing address digits 950-WXXX, the access tandem performs circuit selection based on the WXXX digits.
- If the incoming circuit gives an indication that a continuity check is being performed, the access tandem delays seizure of the outgoing circuit and sets the **Tccr.r** timer and awaits for the continuity message from the end office. At the same time, the access tandem prepares to receive a release message from the end office. When either of these messages are received, the access tandem cancels the **Tccr.r** timer.
- The procedures for the following conditions are discussed later:
 - Expiration of Timers
 - Continuity Check Failure.
- If the COT message indicates that the continuity check was successful or if no continuity check was made, the access tandem seizes the outgoing trunk and waits for a return wink from the IEC.
- When the return wink is received from the IEC, the access tandem performs the following:
 - Generates the address complete message for the incoming circuit and sends it back to the end office.
 - Outpulses the KP + <digits> + ST to the IEC and completes the transmission path. The <digits> refer to the address digits that conform to agreements with the IEC. These may be 950-WXXX, 50-WXXX or 0-WXXX.
 - After outpulsing the address digits, the access tandem waits for the IEC to return an off-hook answer signal on the outgoing circuit. Upon receipt of this signal, the access tandem generates an answer message for

the incoming circuit and returns it to the end office. The answer message causes the end office to provide a carrier connect indication.

10.5.5.4 Four Digit Feature Group B Carriers

Four-Digit Feature Group B Carriers are supported, but access to these carriers is limited to inband signaling trunks.

10.5.6 Feature Group D (FGD) Carrier Identification Code (CIC) Expansion

10.5.6.1 Definition

This feature expands the Carrier Identification Code (CIC) from the current three digits to four digits in the dialing, administration, and signaling formats for FGD and in all other external interfaces and feature interactions.

In order to accommodate a more orderly evolution, the Carrier Access Code (CAC) in the FGD dialing plan expands from five digits to seven digits. The expansion of the CIC from three to four digits modifies the current FGD dialing plan when dialing to override a presubscribed carrier as follows:

- Five-digit carrier access code — 10XXX
- Seven-digit carrier access code — 101XXXX

Currently assigned three-digit CICs will be extended to four digits by prepending the current three-digit code with a 0. For example, a caller currently dials 10XXX at the beginning of dialing in order to reach the carrier from a phone which is not presubscribed to that carrier. The expansion of CIC codes requires the caller to dial 1010XXX to reach the carrier instead.

The interswitch signaling format for FGD includes a CIC whenever the call will be routed from the end office to an interexchange carrier (IEC) via an access tandem or whenever the call uses international signaling. This is true regardless of whether or not the caller is presubscribed to that carrier.

Expanding the CIC also has an impact on many other features and interfaces on the switch. In general, all Operations Systems that either send or receive FGD CICs to/from the switch are affected.

10.5.6.2 Availability

This feature is available in the 5E9(1) and later software releases.

10.5.6.3 Transitional Access Capability

The Transitional Access capability is retained for CICs in the current three digit XXX range (prior to the FGB CIC Expansion), but the administration of assignments and measurements for this capability are slightly modified from the current method.

NOTE: Bellcore is reserving the 10X, 15X, and 16X block of codes for transition purposes, so only 970 are actually available for assignment.

In order for the Transitional Access capability to work, the carrier must get a code assignment for both FGB and FGD, and the FGB code must "map" to the FGD code. (The expansion of FGB CICs, implemented in the FGB CIC Expansion feature, is a prerequisite for this feature.) A Transitional Access carrier with an FGB CIC in the 0XXX or 1XXX range is assigned an FGD CIC of 0XXX. Subscribers are allowed to dial either 950-0XXX or 950-1XXX to reach a Transitional Access carrier, but not both. Regardless of whether 0 or 1 was dialed for this carrier, the call will be considered an FGD call with a CIC of 0XXX, and this will be reflected in the signaling, billing, and measurements

for the call.

10.5.6.4 Switch Engineering

Since this feature is an enhancement to the existing carrier interconnection feature, the engineering considerations for resources in the switch will generally not change. There will be some additional memory required to store carrier translations data and measurements data. The existing carrier interconnect measurements data will continue to be used for engineering purposes. No new measurements will be necessary.

10.5.6.5 Network/Switch Perspective

The capability to support four-digit FGD carrier codes is expected to be deployed network-wide in order to fully use the capability. The switch feature is only part of this larger network capability; other network elements including the Operations Systems (OSs), Application Processors (APs), Service Control Points (SCPs), and Customer Premises Equipments (CPEs) need to be equipped with the software to support the switch feature. A number of steps are required to completely establish the FGD CIC Expansion feature before assignment of four-digit CICs:

- (1) **Split FGB & FGD:** The first step requires that the link between FGB and FGD access types be broken. This is being accomplished by the FGB CIC Expansion feature. This feature should be deployed in each switch that will be upgraded with FGD CIC Expansion along with the accompanying FGB operations systems enhancements.
- (2) **Upgrade OSs, APs, and SCPs:** Step 2 requires that all systems which receive FGD carrier data from the switch be upgraded. This includes FGD-specific modifications on OSs, APs, and SCPs data bases.
- (3) **Upgrade LEC Switches:** The next step requires that the feature be deployed in all equal access switches in the network. When an area is chosen to be upgraded to support FGD CIC Expansion, each switch in that area can be upgraded so long as Steps 1 and 2 have been accomplished for that switch. While it is not essential that the switches in an area be upgraded in a specific order, it is recommended that access tandems be retrofitted first and then subtending end-offices. If the access tandems are upgraded, then trunk signaling conversion can begin as in Step 5 between an end office and the access tandem even if all other end offices have not upgraded. The IEC/INC offices could upgrade at this time if they so desire, but will not be required to do so.
- (4) **Upgrade CPEs:** Step four requires that every affected interface that will send new data to the switch be upgraded with this capability. These interfaces include PBXs.
- (5) **Switch Conversion:** Finally, when all these items are in place, the capability can be phased in separately for the trunk signaling, product interfaces, and dialing.

10.5.6.6 Switch Conversion

10.5.6.6.1 Switch Conversion Introduction

Once each switch has been retrofitted with the four-digit CIC capability, its state can be defined in terms of one of three values: pre-permissive, permissive, or post-permissive.

10.5.6.6.2 Pre-Permissive Period

During the pre-permissive period, only test positions will have the capability to dial the 101XXXX access code and be routed to the proper carrier. It is not recommended that the upgrade of attached systems be delayed beyond the switch upgrade. The reason for this recommendation is because the switch will begin to use four-digit CICs internally as soon as retrofit is complete, and such information would not be accepted by an interface which is only expecting three-digit information.

10.5.6.6.3 Permissive Period

The permissive period begins when the caller is allowed to dial the 101XXXX access code. It is not certain at this point if the permissive period will begin on a nationwide basis, LEC basis, LATA basis, or "area" basis. An area basis may be assumed because the number of retrofits necessary to fully upgrade the whole country is quite large for the period of time allowed. Therefore, it is likely there will be a number of pockets throughout the country which do not have full four-digit capability when the permissive period should be started. The permissive period should be started sometime before the last three digit FGD CIC has been assigned. The switch introduces the permissive period by setting a recent changeable office parameter. During the permissive period, both the 10XXX and 101XXXX dialing formats will be accepted from those switches which have activated the permissive period capability.

10.5.6.6.4 Post-Permissive Period

The permissive period should continue for an indefinite period of time. It is possible that both dialing formats will always be allowed. However, it is anticipated that the telephone companies will require the old format be retired at some point. In order to assign more than 3000 codes, the permissive period needs to end. All systems supporting only three-digit CIC capability which expect to support new carriers must be upgraded by the time the first four-digit CIC is assigned. The telephone company will be able to end the permissive period by simply setting a recent changeable office parameter at the switch. Systems which only wish to support the existing three-digit carriers may still be around after four-digit CICs are assigned at that switch.

10.5.7 Carrier Identification Parameter (CIP)

10.5.7.1 Definition

The Carrier Identification Parameter (CIP) feature allows the delivery of carrier identification codes across the boundary of the originating network.

The delivery of the carrier identification code associated with individual calls allows the consolidation of trunk groups across the network boundary while retaining carrier identification code information.

The carrier identification code associated with each call is carried by a new optional parameter, CIP, in the Initial Address Message (IAM) during call setup. The CIP is delivered to the IEC in a forward direction to indicate one of the following:

- the carrier identification code presubscribed by the call originator,
- the carrier identification code as designated by the originator,
- the carrier identification code response to a number services or intelligent network data base query, or
- the carrier identification code assigned via a digit translation, such as a carrier identification code assigned to a toll-free SAC-NXX or 900-NXX.

LEC switches using directly-connected IEC trunk groups are able to include the CIP in an outgoing IAM on a per-route-index, IEC subscription basis, since the IEC will subscribe to the carrier identification code values on a trunk group basis. Recent change setup is used to allow the recent change routing view to provide independent carrier identification control on a trunk-group basis (View 10.2). This allows independent control of each carrier identification code value for each trunk group. LEC switches using trunk groups to an access tandem for calls involving an IEC will generally include a CIP in each outgoing IAM. The CIP will be available to an IEC for all calls involving an IEC, allowing the access tandem to make a CIP decision for its directly-connected IEC trunk groups. The types of calls include:

- Feature Group D,
- 700 calls
- 900-NXX calls,
- toll-free SAC-NXX calls, and
- toll-free SAC data base calls.

NOTE: International calls are not included.

The Carrier Identification Parameter (CIP) feature is an enhancement to the existing ISDN-UP NI feature.

10.5.7.2 Availability

The CIP feature is a secured feature, available beginning with the 5E8 software release.

10.5.7.3 Feature Application

The CIP feature is provided per carrier identification code value per route. Since the IEC will subscribe to the carrier identification code value on a trunk-group basis, recent change setup is used to allow the routing view to provide independent carrier identification code control on a trunk group basis.

10.5.7.4 System Perspective of Feature Operation

The optional carrier identification parameter contains one of the following:

- the primary carrier identification code presubscribed by the call originator,
- the carrier identification code designated by the originator,
- the carrier identification code response to a number services or intelligent network data base query, or
- the carrier identification code assigned via a digit translation, such as a carrier identification code assigned to a toll-free SAC-NXX or 900-NXX.

If it is sent, the CIP is only included in the outgoing IAM for calls involving an IEC.

A switch, with a directly-connected IEC trunk group, can include the CIP in an outgoing IAM on a per-carrier-identification-code-value per-route basis.

For example, if an IEC is assigned five carrier identification codes for different call services, the different carrier identification code value calls can be configured to terminate to the IEC from a LEC EO or to terminate to the IEC from a LEC AT, all on a single trunk group. When configuring the trunk group, the LEC has the ability to send the CIP for any number of carrier identification codes. The LEC might choose to send the CIP for only two carrier identification codes, in which case the IAM for the other three carrier identification code values would not include the CIP.

For carrier identification code values that route via multiple trunk groups, the individual trunk group level of control can also be achieved.

Within the Equal Access End Office (EAEO), the value used for any CIP depends on what the user dials. See Table 10-6 .

Table 10-6 Values Used In Any Carrier Identification Parameter

If end user dials:	value used in any CIP is:
1+ 7/10 digits (non toll-free SAC or 900 calls)	presubscribed CIC (presubscribed line carrier, IDP group carrier, or office carrier)
10XXX or 101XXXX+7/10 digits (non toll-free SAC or 900 series)	the IXC code dialed (the XXX or XXXX)
a 700 series number	presubscribed CIC (presubscribed line carrier, IDP group carrier, or office carrier)
10XXX or 101XXXX + a 700 series number	the IXC code dialed (XXX or XXXX)
a toll-free SAC-NXX or 900-NXX number, where the switch uses a six-digit translation instead of a database query	the CIC code assigned to the toll-free SAC-NXX or 900-NXX
a toll-free SAC data base call	the CIC code indicated by the SCP in response to the TCAP data base query

10.5.7.5 Engineering

CIP is a secured feature, and arrangements need to be made with Lucent Technologies to activate it.

10.5.7.6 Assignment Dependencies And Limitations

The CIP feature will work as long as there is SS7 on the trunk to the IEC. For instance, there may be inband signaling between an end office and an access tandem, and SS7 signaling between the access tandem and the IEC. See Figure 10-15 .

**Figure 10-15 CIP With Inband Signaling Between An End Office And Access Tandem**

10.5.7.7 Feature Implementation

The CIP feature is implemented via CICIP BLK on RC/V View 8.1.

10.5.7.8 Cross References

The CIP feature number is 99-5E-1526.

10.5.8 Egress - Interexchange Carrier To Local Exchange Carrier

10.5.8.1 Toll Office Initial Address Message (IAM)

After a call has been routed through the IEC network to the terminating toll office, the toll office forms the IAM using the same parameters that were received from the originating toll office. The outgoing IAM toward the LEC does not contain a TNS parameter. The following parameters are passed to the LEC on the basis of the individual ISUP parameter restriction indicators for the outgoing circuit group:

- Calling party number (CPN)
- Charge number
- User-to-user information (UUI)

- Access Transport

NOTE: The User-to-User Information and Access Transport parameters were combined under one parameter in the 5E6 software release and collectively referred to as "Message Associated User-to-User Information" (MA-UUI). One MA-UUI restriction indicator controlled both parameters from the IEC to the LEC network.

In the 5E7 software release, these two parameters were decoupled and each given its own subscription indicator for transport from the originating LEC network to the IEC. Additionally, each parameter has its own restriction indicator to screen each parameter from being passed from the IEC to the terminating LEC network.

Network specific parameters are not passed to the LEC.

10.5.8.2 Call Completion at ISUP End Office or via ISUP Access Tandem

When an IAM is received by an ISUP end office or ISUP access tandem, the called party address is screened. If the called party line is directly served by the office, the switch attempts to complete the call. If the called party line is served by a subtending ISUP end office, the access tandem selects an appropriate circuit to the end office. The procedure for completing the call to the end office is the same as for completing an intranetwork call. The following optional parameters, if received by the access tandem, are included in the IAM sent by the access tandem to the end office:

- Calling party number (CPN)
- Charge number (CHG)
- User-to-user information (UUI)
- Access transport (ATP).

10.5.8.3 Interworking Inband Signaling to ISUP through Terminating Access Tandem

When inband signaling is provided on the trunks between the access tandem and the IEC to interface with ISUP trunks to the end office, the interworking functions at the access tandem are similar to those functions discussed previously.

Upon receiving a seizure from the IEC, the access tandem returns a wink. The access tandem then receives the inband digits from the IxC. The access tandem performs circuit selection to determine if interworking with the ISUP signaling is required.

The procedures for processing the call are the same as those for an intranetwork call with the following exceptions:

- The IAM does not contain a TNS, OLI, or CHG.
- The coding for user service information parameter for 56 kb/s digital data calls, provided under the access tandem procedures for inband to ISUP signaling, is applicable here.

10.5.8.4 Terminating Call Setup ISUP to Inband Signaling Introduction

Figure 10-16 illustrates the interworking for calls coming in from an IEC on ISUP circuit and going out to the end office on a circuit using inband signaling.

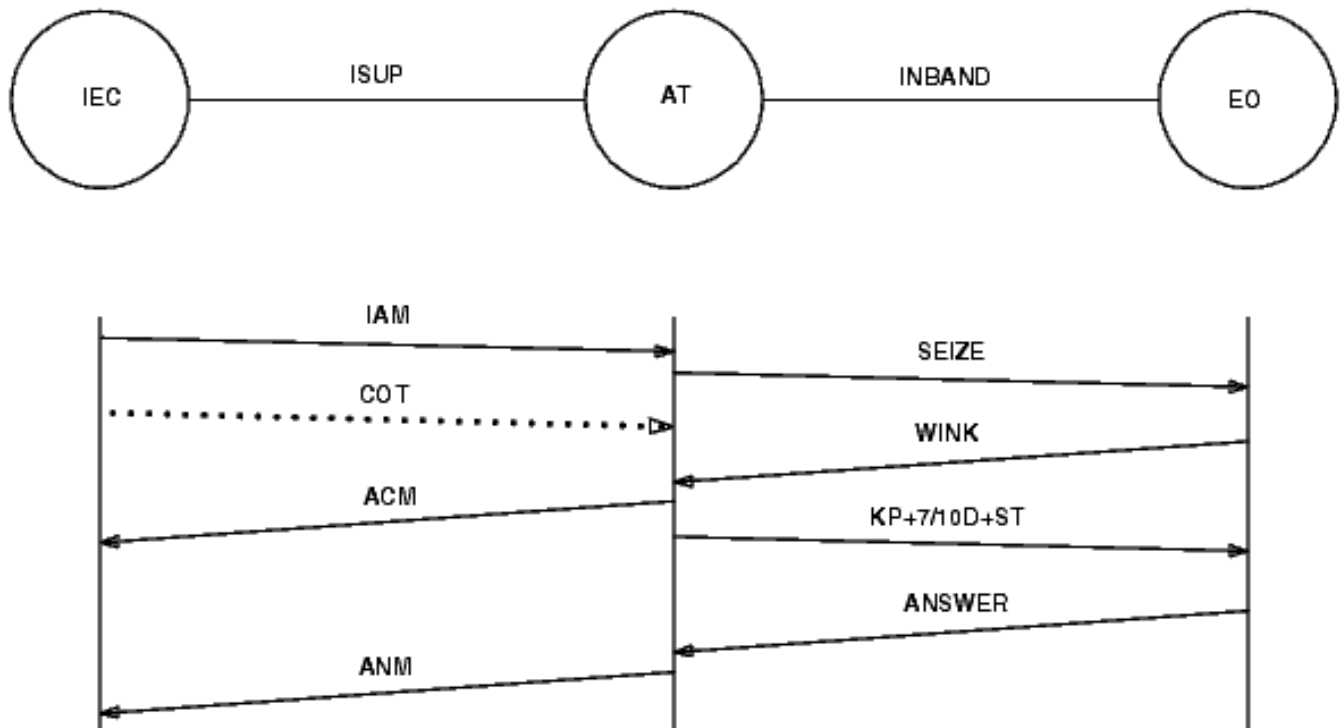


Figure 10-16 Call Setup ISUP to Inband Signaling

For calls to be routed to a subtending end office, the access tandem receives the IAM from the IEC and performs circuit selection based on the following:

- Called number
- Transmission medium requirements in the user service information parameter.

10.5.8.5 Message Associated User-To-User Information

User-to-user information or access transport parameter in any call related messages for incoming ISUP circuits from an IEC interworking to inband signaling is discarded by the access tandem.

10.5.9 Privileged And Corridor Call Handling - High Volume Calls

In areas where a high volume of calls occurs between LATAs, trunking arrangements exist between local area carrier offices in different LATAs. If the local area carrier serves as the default carrier, these calls are referred to as "privileged." If a customer does not specify an IEC to complete the call, the default carrier is used, and where so arranged, the privileged call is established.

If the customer presubscribes to or specifies the particular local area carrier as the selected carrier to set up the call between LATAs, these special trunking arrangements are used. Since the local area carrier is specified, these calls are referred to as "corridor" calls.

10.5.10 Traditional SS7 To A Carrier

This feature gives the operating companies the ability to signal traditional SS7 (TR-NWT-000317) to the carrier while routing based on the NI carrier routing mechanisms. This is attained by placing "traditional" signaling (view 10.2 SIGPRO=TRAD) on SS7 carrier routes and using view 10.3 to select the route index for the carrier based on how

the call was dialed.

Examples of this service are:

- traditional signaling out of carrier route lists to its cellular providers,
- traditional signaling out of carrier route lists for corridor traffic in the Camden, NJ/Philadelphia, PA area, and
- toll-free traffic for private corporate SS7 network which uses carrier routing but TR-NWT-000317 signaling.

To use this capability, the following is required:

- (1) The signaling to the carrier must follow the SS7 TR-NWT-000317 protocol. In other words, the IAM will not contain the NI specific (such as TNS, OLI, etc.) parameters to the carrier.
- (2) The AMA records must contain carrier access times, even though the signaling is based on TR-317. The carrier access record will be updated when the ACM is received (or when the ANM is received, if no ACM is received) from the connecting office and not when the IAM is sent. (The NI direct AMA record is updated when the IAM is sent to the carrier.)

10.5.11 Call Release Message Flow

10.5.11.1 Release Message Location Recoding at Network Interconnect Points

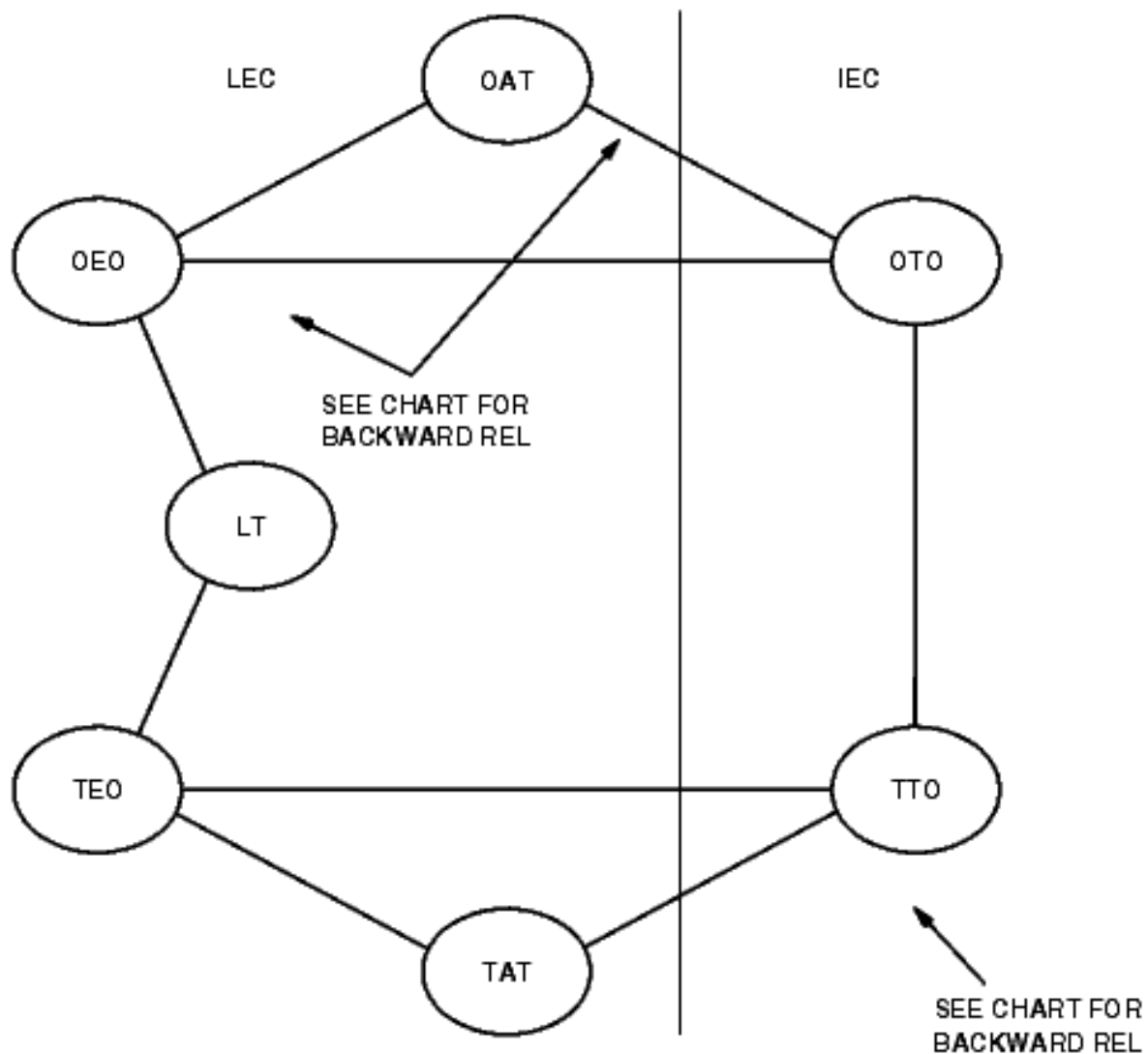
In the 5E6 software release, upon receiving a release (REL) message from a succeeding network, the network boundary switch recodes the cause location value before retransmitting it to the next switch in the network. This is shown in Figure 10-17 .

10.5.11.2 Cause Location Recoding in the 5E7 Software Release

In the 5E7 software release, the cause parameter is supported in two additional messages, *address complete* and *call progress*. In addition, cause location recoding is supported in the forward REL messages. Details are illustrated in Figure 10-18 .

The following constitutes a legend for Figures 10-17 and 10-18 :

User (U)	Unknown (UNKN)
Remote Local Network (RLN)	Remote Private Network (RPN)
Local Local Network (LLC)	Local Private Network (LPN)
Transit Network (TN)	International Network (INTL)
Local Interference Controlled by this Signaling Link (LICTSL)	



OAT = ORIGINATING ACCESS TANDEM
 OEO = ORIGINATING END OFFICE
 LT = LINE TERMINATION
 TEO = TERMINATING END OFFICE
 TAT = TERMINATING ACCESS TANDEM
 TTO = TERMINATING TOLL OFFICE
 OTO = ORIGINATING TOLL OFFICE

CHART		
NO CHANGE		CHANGED VALUES
0000 U	0001 LP	0101 RPN
0011 TN	0010 LL	0100 RLN
0100 RLN	0110 LICTSL	0011 TN
0101 RPN	OTHER	1010 UNKN
0111 INTL		
1010 UNKN		

Figure 10-17 5E6 Software Release Positions for Recoding Cause Location Values

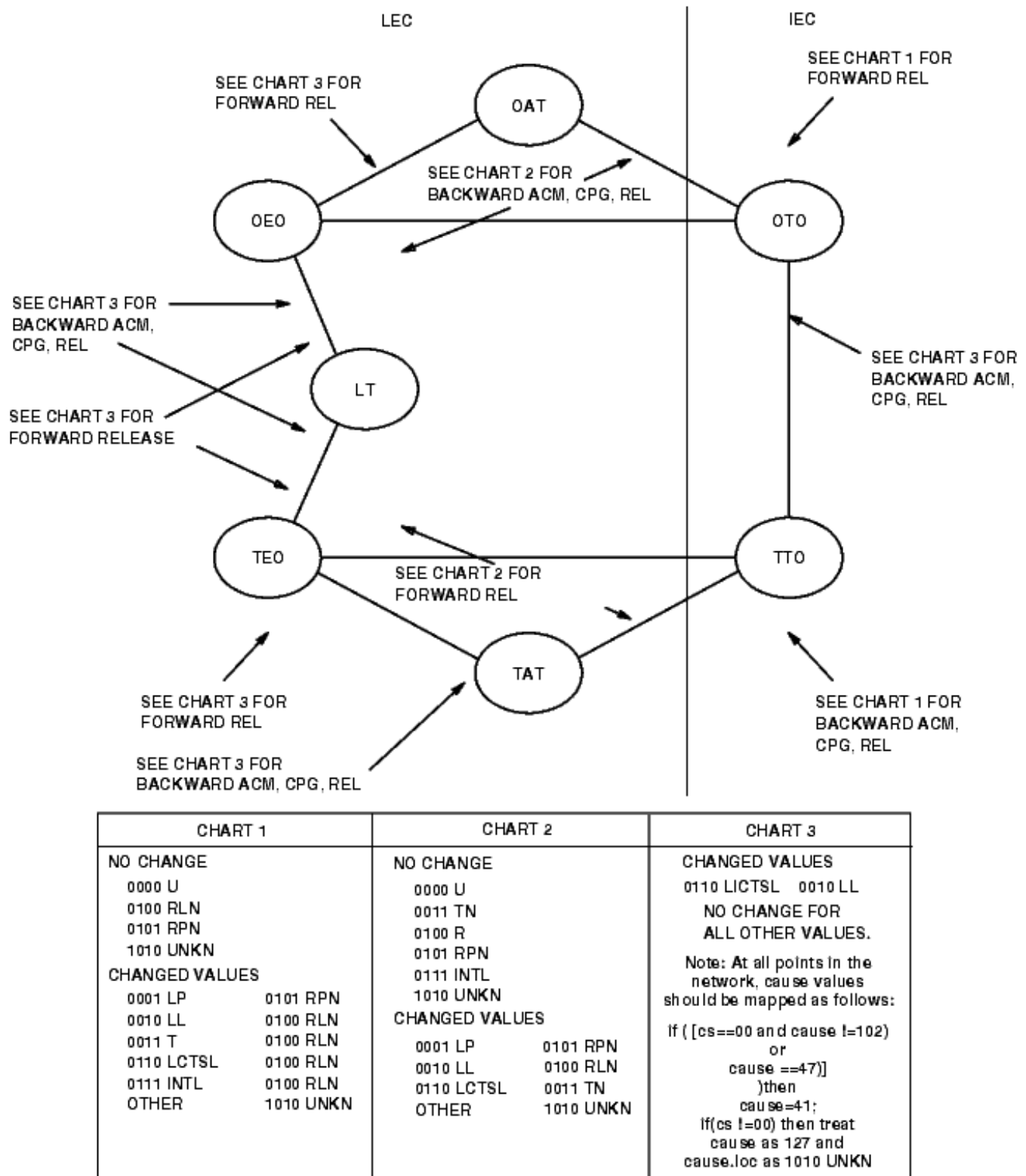


Figure 10-18 5E7 Software Release Positions for Recoding Cause Location Values

10.5.12 Terminating LEC Screening

10.5.12.1 Overview

The procedures for handling screening failures in the 5E6 software release are described in "Problem Causes Signaling Link To Be Declared Failed," Section 5.3.3.

Except for the procedures described in "Called Number Screening Failure," Section 10.5.12.2 and "ISUP Message and Parameter Screening," Section 10.5.12.3, all the procedures for handling screening failures for 5E7 and later software releases are described in "Unsuccessful Call Setup (5E7)," Section 5.3.3.3.

10.5.12.2 Called Number Screening Failure

The method used to determine whether to send a release message or provide a tone/announcement in the case of called number screening failure is changed from that in Phase 1 with regard to internetwork circuits coming into a terminating AT or EO. The use of per-circuit group indicators in Phase 2 replaces the use of the existing per-switch indicator (TR-317). (Also, any per-tone/announcement indicators provided in Phase 1 are overridden by the per-circuit group indicators.) However, this change applies only to called number screening failure.

10.5.12.3 ISUP Message and Parameter Screening

ISUP messages and parameters received at the directly connected end office are verified with respect to reasonable and recognizable signaling information in accordance with ISUP protocol specifications. Messages and parameters received from an IEC in the interval range reserved for intranetwork message and parameter types are discarded.

Network specific values contained within parameter fields of the IAM from the IEC are replaced with the designated default value defined for that field.

If the first office on egress from an IEC receives a TNS parameter with any code value from the IEC in the IAM, the call is cleared. The exchange follows existing procedures for determining whether to release the circuit or play tone/announcement. If a release message is returned, the cause value used is cause value 63, service/option not available, and the location is coded "local local network."

10.5.13 Billing

10.5.13.1 Access Charge - Originating End Office

When the end office originates calls destined for IEC, the carrier connect time depends on whether the call is routed over a direct circuit to the toll office or via an access tandem. If the selected circuit is a direct circuit, the carrier connect time is the time when the IAM is sent to the toll office.

If the call is routed via an access tandem, the carrier connect time is the time that an exit message, an address complete message, or an answer message is received by the end office whichever occurs first. One exception is when a continuity check failure occurs on the connection to the access tandem. If a continuity check failed, an IAM for the same call is sent for a different circuit to the access tandem. If the second circuit does not require a continuity check, or if the continuity check is successful on the second circuit, the carrier connect time is the time that the first exit message, address complete message, or answer message is received for the second circuit. If the continuity check fails on the second circuit, the carrier connect is not achieved.

For Feature Group B calls (950+), the carrier connect time is the time that an answer message is received.

For unsuccessful call attempts caused by timer expiration, incorrect response, or protocol errors, carrier connect time is not achieved. For retries occurring within the interval between the sending of the original IAM and the receipt of an address complete message or answer message for the final circuit, the time duration is considered to be allocated to carrier connect time.

Answer time is the time that an answer message is received at the end office.

Elapsed time from carrier connect time is the time duration measured from carrier connect time until:

- An on-hook is detected from the originating line
- A release message is received
- A release message is sent from the end office.

The elapsed time (from answer) is the time from answer time until:

- An on-hook or ISDN disconnect indicator is detected from the originating line
- A release message is received by the end office
- A release message is sent by the end office.

10.5.13.2 Access Charge - Terminating End Office Access/Tandem

The first office in the terminating LATA to receive the call from the IEC produces AMA records. This may be a directly connected end office or an access tandem.

Carrier connect time is the time the IAM is received by the LEC office without glare or continuity check failure.

Answer time is the time the answer message is received by the local exchange office.

Elapsed time from carrier connect is the time duration measured from carrier connect time until the time a release message is received at the local exchange office or sent from the local exchange office, whichever occurs first.

Elapsed time (from answer) is the time duration measured from answer time until the time a release message is received or sent by the local exchange office.

10.5.13.3 Access Charge - CPN/BN Recording

This section discusses changes to CPN and BN (ANI) access charge recording at an OEO, an end office/service switching point (EO/SSP), or an access tandem/service switching point (AT/SSP). The revised definition of "Table 60" specified in this section affects all call codes and structure codes which currently use "Table 60."

Automatic message accounting (AMA) records are generated by the OEO or AT/SSP for IEC access charging. The originating inter-LATA access record (structure codes 00625, 00626, 00627, and 00628) currently contain "Table 60," ANI indicator, which is now designated as ANI/CPN Indicator and is coded as shown in Table 10-7.

Table 10-7 Table 60 to ANI/CPN Indicator

BCD CHARACTERS	MEANING
1	0 = No ANI or CPN provided 1 = ANI provided, no CPN 2 = CPN provided, no ANI 3 = Both ANI and CPN provided
2	SIGN (hex C)

BCD character 1 of Table 60 is coded as follows:

- "0" if neither ANI nor CPN are provided to the IEC for the call.

There is no change in the use of this code for EAMF calls. For ISUP calls, this case occurs when neither the

charge number nor CPN parameters are included in the outgoing IAM.

- "1" if only ANI is provided to the IEC for the call.

There is no change in the use of this code for EAMF calls. For ISUP calls, this case occurs when only the charge number and originating line information parameters are included in the outgoing IAM. This is true even if the charge number parameter contains no address signal digits. Calling party number parameter is not included in the IAM.

- "2" if only CPN is provided to the IEC for the call.

This code does not apply to EAMF calls. For ISUP calls, this case occurs when only the CPN parameter is included in the outgoing IAM. This is true even if the CPN parameter contains no address signal digits. Neither the charge number nor originating line information parameters are included in the IAM.

- "3" if both ANI and CPN are provided to the IEC for the call.

This code does not apply to EAMF calls. For ISUP calls, this case occurs when the CPN, originating line information, and possibly charge number parameters are included in the outgoing IAM. (The charge number parameter may be omitted if ANI and CPN are identical.) This is true even if the CPN and charge number parameters contain no address signal digits.

10.5.13.4 AMA Record Coding - Route Selection and Trunk Group Number (TGN) Field

10.5.13.4.1 Access Recording

The coding of the first character in the trunk group number (TGN) field, Table 83 of the standard AMA format contains information about the route selected to the IEC. Characters 2 through 5 contain the TGN used to access the IEC if routed directly or, if via an AT, the last SS7 trunk group on the route from the EO to the IEC. Table 10-8 contains access recording information.

Table 10-8 Access Recording

BCD CHARACTER	CODE POINT	MEANING
1	1	Non-CCS7 direct TG
	2	Non-CCS7 EO-AT TG
	3	CCS7 direct TG
	4	CCS7 EO-AT TG with CCS7 AT-IC/INC TG
	5	CCS7 EO-AT TG with non-CCS7 AT-IC/INC TG
2-5		TGN

The 1 and 2 codes do not apply to ISUP trunks. If the call is routed to the IEC on a direct SS7 circuit group, the TGN in characters 2 through 5 will be that of this direct circuit group, and character 1 will be coded "CCS7 direct TG" (3).

If the call is routed to the IEC via an AT on SS7 circuits between the EO and AT and also between the AT and IEC, the TGN in character 2 through 5 will be the circuit group number between the AT and the IEC. The coding of character 1 will be "CCS7 EO-AT TG with SS7 AT-IC/INC TG" (4).

If the call is routed to the IEC via an AT on SS7 circuits between the EO and AT and non-SS7 between the AT and the IEC, the TGN in characters 2 through 5 will be the circuit group number between the EO and the AT. The coding of character 1 will be "CCS7 EO-AT TG with non-CCS7 AT-IC/INC TG" (5).

10.5.13.4.2 Egress Recording

The coding of the first character in the trunk group number (TGN) field, Table 83 of the standard AMA format contains information about the trunk used to route from the IEC directly to the EO or to the AT. Table 10-9 contains access recording information.

Table 10-9 Egress Recording

BCD CHARACTER	CODE POINT	MEANING
1	1	Non-CCS7 direct TG
	2	Non-CCS7 EO-AT TG (with non-CCS7 AT-IC/INC TG)
	3	CCS7 direct TG
	4	CCS7 EO-AT TG with CCS7 AT-IC/INC TG
	5	CCS7 EO-AT TG with non-CCS7 AT-IC/INC TG
	6	Non-CCS7 EO-AT TG with CCS7 AT-IC/INC TG
2-5		TGN

The TGN will identify the trunk used to route from the IEC directly to the EO or AT.

The 1 and 2 codes do not apply to ISUP. If the call is routed from the IEC to the EO on a direct SS7 trunk, character 1 is coded "CCS7 direct TG" (3).

If the call is routed from the IEC via an AT to the EO on all SS7 supported circuit groups, character 1 is coded "CCS7 EO-AT TG with CCS7 AT-IC/INC TG" (4).

If the call is routed from the IEC to an AT on a MF trunk group but then interworked to an SS7 circuit group to the EO, character 1 is coded "CCS7 EO-AT TG with non-CCS7 AT-IC/INC TG" (5).

If the call is routed from the IEC to an AT on an SS7 circuit group but then interworked to an MF trunk group to the EO, character 1 is coded "Non-CCS7 EO-AT TG with CCS7 AT-IC/INC TG" (6).

10.5.13.5 Billing References

For detailed billing information, see 235-190-300, *Billing Features and Specifications*.

10.5.14 Administration

10.5.14.1 Administration Introduction

On site switch personnel, in conjunction with local support systems and remotely located work centers, monitor the overall operation stability of the switch and the network.

Administration of the data and report structures concerning network interconnect are handled by specific methods for switch handling for specific services. All data formatting and report generation is accomplished by the switch resources and operational support systems.

10.5.14.2 Maintenance Measurements

Measurements necessary to support the day-to-day maintenance efforts for network interconnect are required. These measurements are generated, collected, and analyzed by both on-site work forces at the switch locations and by centrally located support centers.

More detailed information on ISUP measurements and reports can be found in 235-070-100, *Administration and Engineering*.

10.5.14.3 Office Data

Table 10-10 contains the office data items and the basis for their provisioning.

Table 10-10 Office Data Summary

INDICATOR	DEFAULT VALUE	PROVISIONING BASIS	
		END OFFICE ^a	ACCESS TANDEM
Privacy	Not Private	Customer	
Charge Information Subscription	Not Subscribed	IEC	
Calling Party Number Subscription	Not Subscribed	IEC	
ANI Privacy	Not Private		Incoming EA/MF or CAMA TG
Dual Seizure Control	Odd/Even	ISUP CG	ISUP CG
All/None Control		ISUP CG	ISUP CG
Calling Party Number Restriction	Do Not Pass		
Orig Line Info Restriction	Do Not Pass		
ATP Restriction	Do Not Pass/ Discard	ISUP NI CG	ISUP NI CG
UUI Restriction	Do Not Pass/ Discard	ISUP NI CG	ISUP NI CG
Tone/Announcement Procedure ^b	Return REL	Office	Office
Tone/Announcement Required	c		

Legend:

The following are definitions of terms used in this table:

CAMA TG Centralized Automatic Message Accounting Trunk Group

ISUP CG Signaling System 7 Circuit Group

ISUP IN CG Signaling System 7 Interconnect Circuit Group

EA/MF Exchange Access Multifrequency

IEC Inter-LATA or International carrier

ANI Automatic Number Identification

ATP Access Transport Parameter

UUI User-to-User Information

Notes:

a. This may be an Access Tandem that directly serves customers.

b. Existing intranetwork indicator.

c. For international announcements, the default value is "required." For all other calls, the default value is "not required."

10.5.14.4 Timing and Tolerances

There are various timers associated with the ISUP call setup and release procedures. These are the same as those for intranetwork calls. Table 5.6-2 shows the timers particular to ISUP calls along with their allowable ranges.

11. ISUP/TCAP RELATED FEATURES

11.1 INTERMODULE TRUNKING

11.1.1 Availability

Intermodule Trunking is available with the 5E7 software release.

11.1.2 Description

The Intermodule Trunking (IMT) feature provides direct trunking between modules connected to a 5ESS®-2000 switch.

NOTE: Single-SM loop-around trunks (intramodule trunks) are described in Sections 11.2 and 11.3 .

The types of modules that support IMTs are multimodule remote switching modules (MMRSMs), optically integrated remote switching modules (ORMs), remote switching modules (RSMs), switching modules (SMs) and two mile optically integrated remote switching modules (TRMs). The IMTs can be designated as the primary route (linked or stand-alone operation) with the network control and timing (NCT) links as an optional overflow route, or they may be designated as an emergency route to the NCT links (stand-alone operation only). Additionally, alternate and/or primary routes could be specified with the capability to tandem switch traffic through IMTs in combination with other IMTs or trunks attached to modules connected to a switch.

The routing capabilities of IMTs are dependent on the type of signaling provided. The IMTs may use either traditional signaling or Integrated Services Digital Network User Part (ISUP) signaling. Trunks using traditional signaling, which encompasses inband trunk signaling [such as multifrequency (MF)] function during both linked and stand-alone operation. In contrast, IMTs using ISUP signaling, which is used exclusively by Signaling System 7 (SS7) trunks, only function during linked operation. The IMTs support circuit-switched traffic, Business and Residence Custom Services (BRCS) features and other interoffice features currently supported by trunking arrangements. Additionally, SS7 IMTs support Local Area Signaling Service (LASS) features.

The network goal of IMTs, beyond providing direct trunking, is to increase reliability by providing an alternate link for routing traffic to and from (remote) switching modules connected to a switch. Also, IMTs could be incorporated to carry traffic over existing trunk facilities when community dial offices (CDOs) are replaced by MMRSMs connected to a switch to unload the T1 umbilicals when heavy traffic is expected between MMRSMs. Finally, IMTs may be used to avoid crossing LATA boundaries when the switch and remote switching modules are in different local access transport area (LATAs).

11.1.3 Configuration Types/Module Compatibility

The IMT feature allows for the direct interfacing of the different types of modules, common to a switch, with the use of peripheral trunking facilities. These trunking facilities may be analog or digital. The possible combinations of module types are illustrated in Figure 11.1-1 , and listed in Table 11.1-1 .

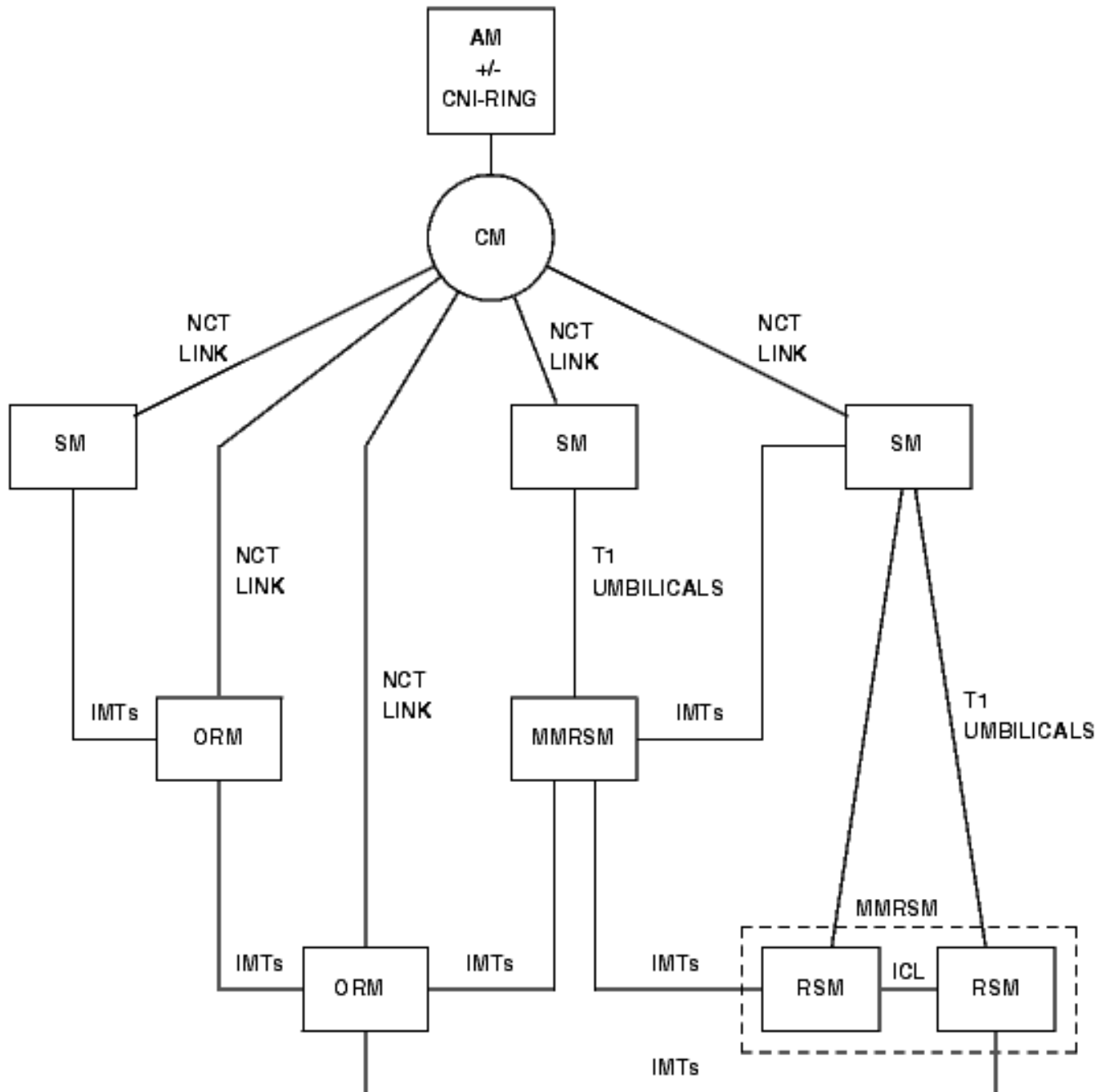


Figure 11.1-1 Module Compatibility for IMTs

NOTE: In Figure 11.1-1, the TRM and the single RSM are not shown in any of the possible module combinations. This was done to avoid complicating the diagram. However, these two module types are indirectly shown in the diagram. The TRM, which is an ORM with a two mile restriction, could be incorporated into the diagram by replacing any module identified as an ORM, and the single RSM, which is a single module MMRSM, could also be incorporated into the diagram by replacing any module identified as an MMRSM. Therefore, all the possible module combinations for IMTs have been displayed in the diagram.

Table 11.1-1 Module Compatibility

MODULE	MMRSM	ORM	RSM	SM	TRM
MMRSM	Yes	Yes	Yes	Yes	Yes
ORM	Yes	Yes	Yes	Yes	Yes
RSM	Yes	Yes	Yes ^a	Yes	Yes
SM	Yes	Yes	Yes	Yes ^b	Yes
TRM	Yes	Yes	Yes	Yes	Yes
Notes:					
a. See Section 11.1.11 , Restrictions and Limitations, Item 4.					
b. See Section 11.1.11 , Restrictions and Limitations, Item 12.					

11.1.4 Routing Capability

The ability to route through IMTs is dependent on the operational state of the modules involved. The two types of operational states are linked and stand alone. Linked operation is the normal state for all types of modules. This state requires a module to have communications with the AM through an NCT link and/or T1 umbilical. The IMTs using either SS7 or traditional signaling function in this state. On the other hand, stand-alone operation is an abnormal state for all types of modules. In this state, a module has lost communications with the AM because of the loss of an NCT link and/or T1 umbilical. During stand-alone operation, only IMTs using traditional signaling in those modules equipped with the stand-alone feature function. The possible options available for routing traffic over IMTs are in the following sections.

11.1.5 Primary IMTs With Secondary NCT Links

11.1.5.1 Primary IMTs With NCT Links Blocked

Use the IMTs as the primary route and disallow overflow or alternate routing to the NCT links. See Figure 11.1-2 . The (a) route is the only route between the modules. The (b) route is blocked as an overflow route.

11.1.5.2 Emergency IMTs

Use the NCT links as the primary route and route through the IMTs only when one or more of the modules are in stand-alone operation. See Figure 11.1-2 . The (b) route is the only active route during linked operation, while the (a) route is the emergency route that becomes operational only when one or more of the modules enters a stand-alone state. This configuration type can only be used when the modules are equipped with the stand-alone feature and when the trunks between the modules are using traditional signaling.

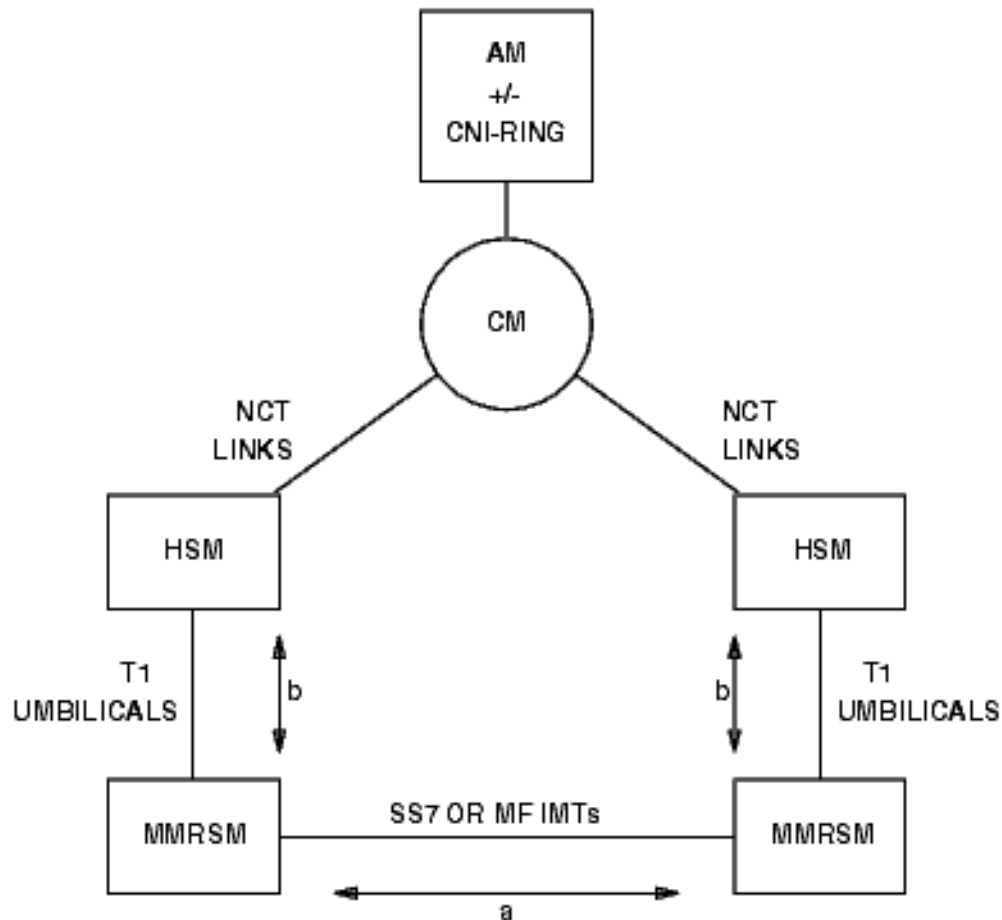


Figure 11.1-2 Basic IMT Configuration

11.1.5.3 Primary Tandem IMTs

Use the IMTs for tandem routing intermodule traffic through another module acting as a tandem switch. See Figure 11.1-3. The (a) route is the primary route between modules directly connected with IMTs. The (c) route is the primary route between modules indirectly connected with IMTs, and the (b) route is the possible overflow route for the (a) and/or (c) route.

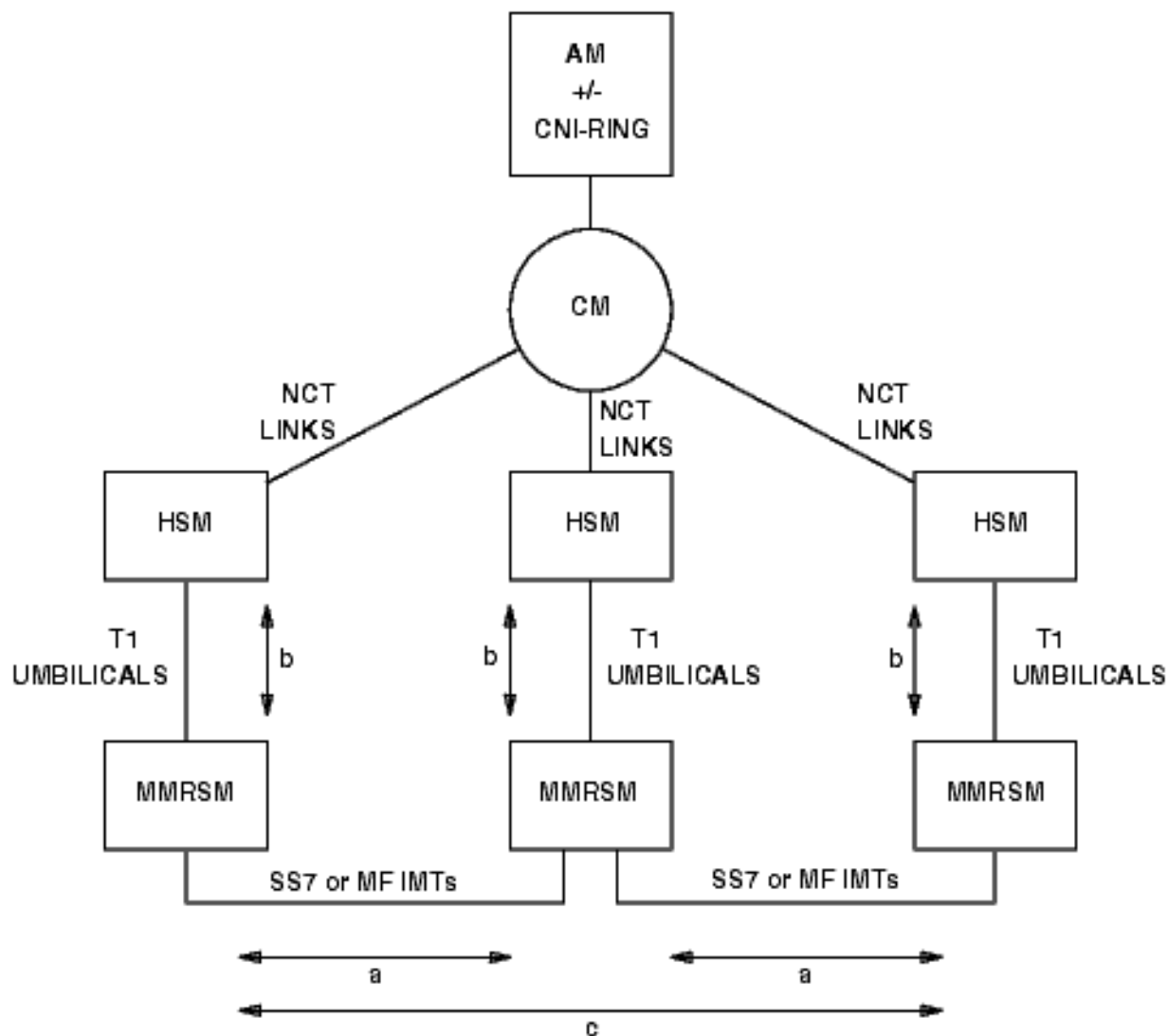


Figure 11.1-3 IMT Configuration Using Tandem Routing

11.1.5.4 Secondary Tandem IMTs

Use the IMTs, which directly connect modules together, as the primary route and use those, which indirectly connect modules together, as an alternate route. In addition, the NCT links could be used as a second alternate route to supplement the tandem IMTs. See Figure 11.1-4. The (a1), (a2), and (a3) routes are the primary routes between the modules, and the (a1-a2), (a1-a3), and (a2-a3) routes are the alternate routes. Also, the (b) route could be used as a second alternate route to the (a#-a#) routes. This configuration would allow traffic to overflow from the (a#) routes to the (a#-a#) routes and finally to the (b) route, if necessary.

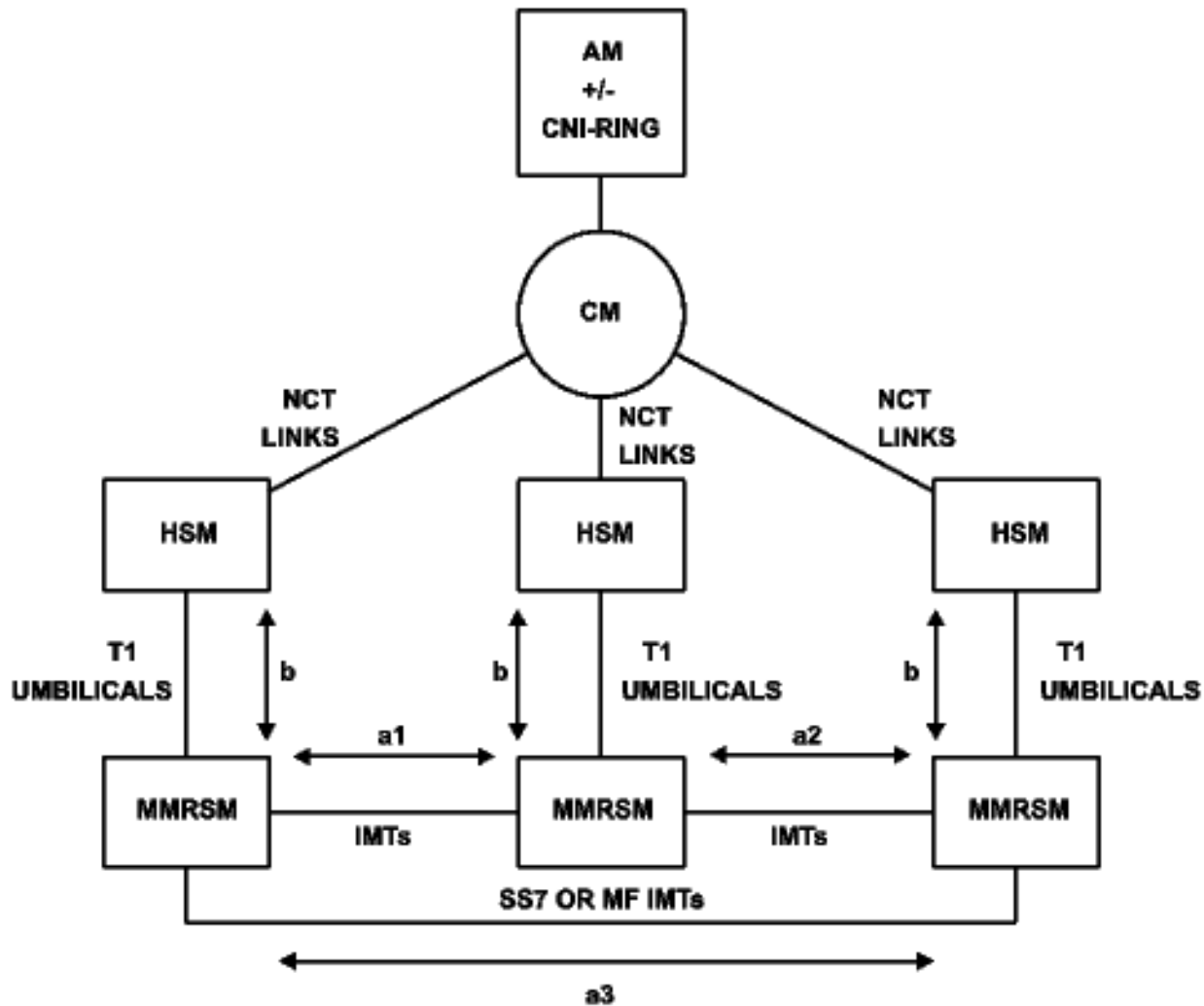


Figure 11.1-4 IMT Configuration Using Overflow Tandem Routing

11.1.5.5 SS7 IMTs with Emergency MF IMTs

Use the SS7 IMTs and the NCT links as prescribed by the aforementioned routing options in "Primary Tandem IMTs," Section 11.1.5.3, or "Secondary Tandem IMTs," Section 11.1.5.4. In addition, the MF IMTs would be used as an emergency route during stand-alone operation. See Figure 11.1-5. The (a) and (b) routes follow the configurations stated in routing options in "Primary Tandem IMTs," Section 11.1.5.3 or "Secondary Tandem IMTs," Section 11.1.5.4. The (c) route is the emergency route, which becomes operational only when one or more of the modules enters a stand-alone state. This route only functions when the modules are equipped with the stand-alone feature and the IMTs are using traditional signaling.

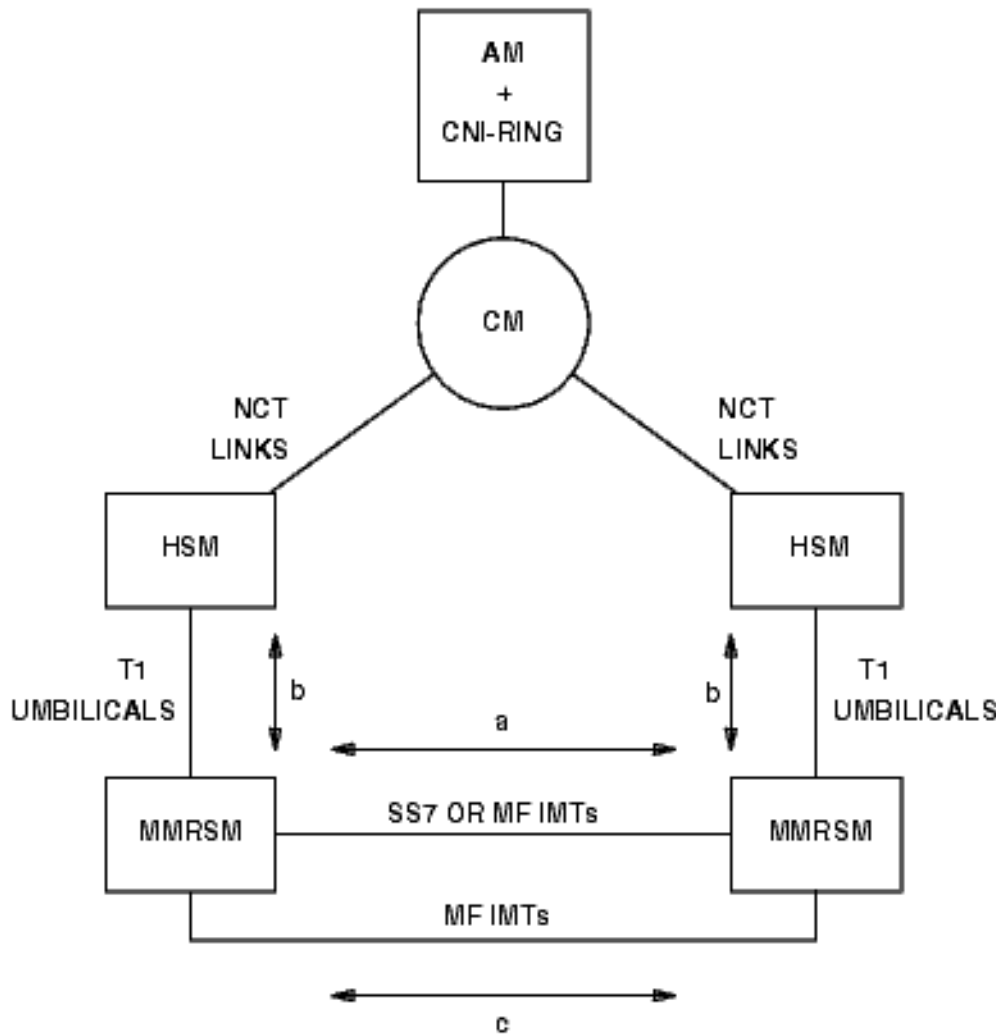


Figure 11.1-5 IMT Configuration Using Two Types of Signaling

11.1.6 Feature Interactions

The IMTs support POTs traffic, BRCS features and other interoffice features currently supported by the other types of trunking arrangements. In addition, SS7 IMTs support LASS features. The capabilities for some features, however, are not always functionally identical when they are used over IMTs instead of another trunking arrangement. These differences are identified in "Restrictions and Limitations," Section 11.1.11.

11.1.7 Trunk Administration/AMA Billing Treatment

Rating intermodule traffic, which is the responsibility of the telephone company, is based on the distance and the tariff structure independent of the actual routing used. Whether the traffic was actually routed through the NCT links or through the IMTs, normal AMA treatment is used for charging the customers.

11.1.8 Call Trace

The In Progress Call Trace (IPCT), the Nuisance Call Trace (NCT), and the Utility Call Trace (UCT) are capable of tracing both ends of any intra-office call, including those that traverse IMTs. Call traces can be processed from, through, and to an IMT using both the directory number and the trunk information. Call trace does not function on any module that does not have communications with the AM.

11.1.8.1 Busy-Idle State of Trunks

Customer complaints about service may require that operating company personnel be able to display the dynamic channel occupancy of a given T1 facility. Such information may reveal why incoming wide band calls are being blocked; the UCT display provides a view of available channels and also shows the traffic that is present.

The UCT will show the end-to-end view of a single channel of a wide band call. Traces can be triggered off of trunk group and member number, port, equipment number or network time slot. The path of the traced channel will be determined and the far end path corresponding to the traced channel will also be displayed. Traces triggered off of process IDs will display the master channel of the wide band call only.

The `OP:CHANMAP` command is provided as a front-end for the UCT mechanism. A user could use `OP:CHANMAP` to determine which channel is of interest and then perform a UCT on that channel to find the needed information about the complete path through the switch. The `OP:CHANMAP` is an easy way to see what time slots were chosen by path hunt software and also provides a way to display how trunk hunt set up the trunks for a particular call.

The `OP:CHANMAP` also provides a convenient way to see how many calls are present on a facility (the busy idle status of all trunks members on a particular facility). The UCT is also used in the field to see how a call goes through the network. This is especially helpful to someone who is trying to install a new service and wants to know if they have correct routing data.

11.1.9 Traffic Measurements

Traffic measurements for intermodule calls through IMTs are provided as part of Section 12 of the switch 30-Minute Traffic Report through the following trunk group counts:

- Incoming Peg Count and Usage Count
- Outgoing Peg Count and Usage Count
- Maintenance Usage Count
- Overflow Peg Count.

From an office standpoint, an intermodule call through an IMT is viewed as two calls because two modules switch the same call as compared to a call switched by the CM through the NCT links. Additionally, if features are used over the IMTs, the associated 30-Minute Traffic Report is treated normally and receives a peg count and usage count.

11.1.10 Trunk Maintenance

Trunk maintenance for an IMT is equivalent to the standard maintenance performed on other trunking arrangements. The major trunk tests included as part of the standard maintenance tests are described later.

Trunk tests for IMTs, available through the integrated services test facility (ISTF), the trunk test facility (TTF), and the directly connected trunk unit (DCTU), function when the modules, which are connected to the IMTs, have communications with the switch. However, a remote module that is in a stand-alone state is not able to use ISTF, TTF, and DCTU test capabilities. Automatic routine maintenance tests, which use the automatic process testing (APT) capabilities, function over IMTs to ensure that these trunks operate when needed. The APT provides the continuity check for IMTs to test the integrity of the trunk hardware and verify that the tuples in the relation `RLIMTTRKS` agree with the physical connections. Additionally, SS7 IMTs have the capability to use voice path assurance (VPA) testing during linked operation. During these tests, outgoing IMTs on one module is considered as incoming trunks on the other module.

An intermodule call, as part of the IMT tests, is not alternate routed, if the alternate route option is being used. Also, the test is treated as two calls. Therefore, trouble detection and notification are consistent with the standard types used by the other trunking arrangements. This implies that failure messages, (such as, CGAs and MDIIs) are generated by both modules connected to the IMT and displayed at the master control center (MCC) and/or trunk and line work station (TLWS) even though the messages refer to the same trunk.

11.1.11 Restrictions and Limitations

The following limitations and restrictions apply:

- (1) SS7 IMTs require ISUP signaling. Additionally, both modules common to the IMTs are required to maintain communications with the AM and/or direct link node (DLN) through the NCT links and/or the T1 umbilicals in order for the IMTs to function.
- (2) SS7 features (including LASS) and BRCS traffic that use ISUP signaling do not function over IMTs unless the modules, which terminate the IMTs, have communications with the AM and/or DLN.
- (3) LASS features do not function consistently over IMTs between two modules unless 100 percent of the active IMTs are using ISUP signaling.
- (4) In an MMRSRM, IMTs between the RSM members of the multimodule are not implemented. The RSMs within an MMRSRM are interconnected by inter-RSM communications links (ICLs), which are considered internal to the switch. If both ICLs and IMTs were allowed in an MMRSRM, a conflict between the internal and peripheral routes would result.
- (5) 64 kb/s clear channel capability does not function when one or both of the modules, which terminate the IMTs, are in stand-alone operation.
- (6) The MMRSMs and RSMs which use IMTs require the use of additional peripheral time slots within the remote module; however, an equivalent number of time slots become available in the host module. This configuration exchanges the traffic capacity between the host module and the remote module.
- (7) The designation of the NCT links as the primary route and the IMTs as the alternate route is not an available routing configuration.
- (8) In order for IMTs using traditional signaling to function during a stand-alone operation, the modules must have the stand-alone call processing feature available.
- (9) During a module overload condition, there is no available mechanism to throttle IMT traffic from routing to the overloaded module.
- (10) Module combinations including ORMs, SMs, and/or TRMs that use IMTs for routing require the use of additional peripheral time slots in comparison to using the NCT links for routing.
- (11) The IMTs is used between two SMs. Even though the IMT feature allows this configuration, there is no advantage, due to SM proximity, because additional peripheral time slots are required at the SMs when routing through IMTs in comparison to routing through the NCT links.
- (12) The ability to tandem traffic through IMTs to operators services position system (OSPS) or traffic services position system (TSPS) does not function.
- (13) Packet-Switched Data (PSD) does not function on intermodule digital trunks.
- (14) More real time is needed to process a call through an IMT compared to a call being routed through the NCT links and/or T1 umbilicals. This is a direct result of the additional processing required within the individual modules.

- (15) Remote testing units, such as the DCTU, cannot be shared among modules through the IMTs.
- (16) Conference call features do not function over IMTs unless the terminals involved have access to GDSU resources.
- (17) Traffic is not allowed to loopback through IMTs.

11.1.12 Translation Requirements

The translation requirements for IMTs follow nearly all the guidelines and rules typically used by other trunking arrangements. Consequently, only the areas in translations that contain additional guidelines and/or rules, specifically for IMTs, are discussed in this section.

In addition, IMT translations are required in every module connected to an IMT as if each module were an independent switch. The RCV views necessary to incorporate the translations for primary and/or emergency routed IMTs are shown in Tables 11.1-2 and 11.1-3 .

Table 11.1-2 Primary IMT Provisioning

VIEW	DESCRIPTION
5.1	Trunk Group
5.5	Trunk Member
5.46	Inter-SM Trunking
10.2	Route Index
9.1	Digit Analysis Selector
9.3	Local Digit
9.5	Incoming Trunk Preliminary Digit
9.25	LDIT and Associated SM List
4.1	Line Class Code

Table 11.1-3 Emergency IMT Provisioning

VIEW	DESCRIPTION
5.1	Trunk Group
5.5	Trunk Member
5.46	Inter-SM Trunking
10.2	Route Index
4.9	Emergency TN Assignments

11.1.12.1 Trunk Translations

11.1.12.1.1 RCV 5.1 - Trunk Group

The translations required for a trunk group are consistent between IMTs and other types of trunking arrangements. This also includes translations necessary for either ISUP or traditional trunk signaling.

DEST PT CODE - The destination point code identifies the signaling point for which a CCS message is intended. This field is required only for IMTs using ISUP signaling. The destination point code is illustrated in Table 11.1-4 .

Table 11.1-4 Destination Point Code

NETWORK INDICATOR	NEAR-END SM NUMBER	FAR-END SM NUMBER
000	001-192, 255 ^a	001-192, 255 ^a
Notes:		
a. The value 255 indicates a loop-around trunk on a single SM. See Sections 11.2 and 11.3		

ORIG PT CODE - The originating point code identifies the signaling point that is the source of a CCS message. This field is required only for IMTs using ISUP signaling. This entry is identical to the local point code of the switch that

contains the IMTs.

INTER SM TRK - The inter-SM trunk field identifies intermodule trunk groups. This field is set to a "Y" for an IMT using either traditional or ISUP signaling; otherwise, the field is set to the default of "N" which is used to indicate any other type of trunking arrangement.

11.1.12.1.2 RCV 5.5 - Trunk Member

The translations required for trunk group members are identical in comparison between IMTs and other types of trunking arrangements. Additionally, these translations are dependent on the signaling type being used by the trunk group, respectively. For example, an SS7 IMT group member is translated in the same manner as a typical SS7 trunk group member.

11.1.12.1.3 RCV 5.46 - Inter-SM Trunking

The translations for this form are required, exclusively, for IMTs. This form defines the IMT connections and provides information about both ends of the trunk. The originating and terminating ends of an IMT are relative to the vantage point of a specific module.

- SM - The SM field is used to identify the SM number from which an IMT is originated. The valid range of entries is 1-192.
- TGN - The trunk group number field identifies the originating end of an IMT group. The valid range of entries is 1-2000.
- MEMB - The member number field identifies the originating end of an IMT group member. The valid range of entries is 0-1951.
- MATE SM - The mate SM field is used to identify the SM number to which an IMT is terminated. The valid range of entries is 1-192.
- MATE TGN - The mate trunk group number field identifies the terminating end of an IMT group. The valid range of entries is 1-2000.
- MATE MEMB - The mate member number field identifies the terminating end of an IMT group member. The valid range of entries is 0-1951.

11.1.12.2 Routing Translations

11.1.12.2.1 RCV 9.25 - LDIT and Associated SM List

The additional digit analysis translations required for IMT routing between two modules would waste memory space if they were stored throughout a switch; therefore, a module based local digit interpreter table (LDIT) was introduced. This form is used to associate module(s) with a particular LDIT value. This allows LDIT information to reside only on the specific module(s) which require the information, thereby, optimizing the usage of module memory.

- LDIT - The local digit interpretation table field identifies the LDIT number associated with the digit analysis translations used for IMT routing. The valid range of entries is 1-999.
- LIST OF SWITCHING MODULES - The list of switching modules field may contain 192 subfields. This field contains a list of modules that are associated with the indicated LDIT. The valid range of entries is 1-192.

11.1.12.2.2 RCV 10.2 - Route Index

The translations required for the route index are dependent on the configuration option selected. The route index is used to define the routing of traffic. The route index for the IMT is defined to be almost identical to any other traffic carrying trunk arrangement except for one additional option. This option would allow an IMT primary route to have an alternate route through the NCT links.

- **ETYP** - The route type field defines the type of routing treatment that is used. For an IMT, the route index is defined with a routing treatment of "HUNT," and the alternate route index is defined with a routing treatment of "DNTRAN." The "HUNT" value allows the IMT group to search for an idle IMT group member, while the "DNTRAN" value allows traffic to alternate route over the NCT links if an idle IMT group member cannot be found.
- **NEXT RTI** - The next route defines the alternate route index when the route type contains a value of "HUNT." If the route type is "DNTRAN," then an NOC is entered. Finally, if a true alternate route index is not required, the next route index number is omitted and reorder is automatically provided on overflow.

11.1.12.3 Line Translations/RCV 4.9 - Emergency TN Assignments

The ability to route traffic during a module isolation state over emergency IMTs, which use traditional signaling, can be provided with this RCV form. The translations required to accomplish this optional routing are defined as follows.

- **REMOTE SITE** - The remote switching module number identifies the module that requires emergency routing capabilities. This field is only populated when an MMRSM, an ORM, an RSM, or a TRM is used. The valid range of entries is 1-174.
- **LOCAL SM** - The local switching module number identifies the module that requires emergency routing capabilities. This field is only populated when an SM is used. The valid range of entries is 1-192.
- **EMER TN** - The emergency telephone number field indicates a telephone number or range of telephone numbers not served by the remote site or local SM that is rerouted to an outgoing IMT when the module is in a stand-alone state. To specify a range of telephone numbers, use the wild-card character (*). Possible entries using the wild-card character are as follows:

XXX-XX**:	Reroute a hundreds group to the same alternate destination.
XXX-XXX-XX**:	
XXX-****:	Reroute an entire office code to the same alternate destination.
XXX-XXX-****:	
-*:	Reroute all office codes within an area code to the alternate destination.
XXX-***-****:	
*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*:	Reroute all dialed calls (up to 15 digits) to the same destination.

The X is a value 0-9. The wild-card (*) character matches any dialed digit at that position. This field is used to populate the `RT_EMRNM` relation.

When determining the order of precedence for matching emergency routing DN's, if an exact match fails on the entire DN, then partial matches are attempted with wild card (*) digits in the hundreds group, in the whole office code, in the entire area code, and lastly for all 15 digits.

A range of telephone numbers specified with a wild-card character must not overlap another range of telephone numbers for a remote site or local SM in this relation. If an overlap occurs and the modules connecting the IMTs are in stand alone, a routed number that is overlapped would appear to terminate in both modules. This would result in the number looping through all the members of the IMT group until it is blocked.

The software was modified to give reorder instead of emergency routing after a call has been routed to a fixed

route or announcement trunk. For example, this would occur when a mis-dialed call to an unassigned DN accesses the routing module for that number. Calls to the Operator or 911 that would have terminated to announcement because of a stand alone condition are allowed to emergency alternate route.

Stand-Alone Test Lines allow testing of emergency number rerouting for a RSM/ORM/SM site when the RSM/ORM/SM site is not in stand-alone mode. The lines must have a LINE CLASS CODE (LCC) with a SERVICE CLASS of "SATSTLN" and a TERMINATING TREATMENT of "INDIV." When conducting the stand-alone rerouting test from the RSM/ORM/SM Site, the lines may be used to originate and dial each of the emergency numbers which is normally rerouted during stand-alone operation.

- PREFIX - The prefix field indicates the prefix dialed with the emergency number. This field always contains the default value "NONE" when this form is being used with emergency IMTs.
- ALT TN - The alternate telephone number field is left blank when this form is being used to route traffic to an emergency IMT; otherwise, the RCV cross-checks do not allow a route index for an IMT to be indicated.
- RI - The route index field indicates the route index associated with the outgoing IMT group to which the traffic is routed instead of the normal routing associated with the telephone number or range of telephone numbers identified by the EMER TN field. The valid range of entries is 1-3617.
- OUTPULSED DIGITS - The outpulsed digits field identifies the number to be outpulsed over an IMT group. This field is left blank, thereby, allowing the telephone number or range of telephone numbers indicated in the EMER TN field to be outpulsed over an emergency IMT group.

11.1.12.4 Engineering Assignments - RCV 18.1 - Switching Module

In order for the emergency IMTs that use traditional signaling to function, the stand-alone call processing feature is available to the modules that terminate the ends of the IMTs. The availability of the feature to the modules can be found on this RCV form. The field is identified as STAND-ALONE SM. This field has the value of "Y" if the stand-alone feature is equipped on the module, allowing emergency IMTs to function in an isolated state. A value of "N" indicates that the feature is not equipped, preventing emergency IMTs from functioning in an isolated state.

11.2 PSU-BASED INTRAMODULE TRUNKING

11.2.1 Description

The VCDX Loop-around Intramodule Trunk feature, 99-5E-4360, implements loop-around SS7 trunks to offer local and long distance applications on VCDX switches and single-SM 5ESS[®]-2000 switches.

For CNI-based intramodule trunking, see Section 11.3 .

11.2.2 Availability

The VCDX Loop-around Intramodule Trunk feature is available as a software update for 5E12 and is included in 5E13 and later software releases.

11.2.3 Environment

The VCDX Loop-around Intramodule Trunk feature is implemented on 5ESS[®]-2000 switch Very Compact Digital Exchange (VCDX) switches equipped with SM-2000s and single-SM 5ESS[®]-2000 switches. The feature is *not* implemented on the 5ESS[®]-2000 switch (see Section 11.3), on VCDX switches with SMs, or for wireless applications.

11.2.4 Cross References

The following cross references apply to this feature:

- Feature Number: 99-5E-4360

11.2.5 Background

Because there is not full interworking between local and long distance software platforms (a call originating on a line cannot access the ANI table), a single call that uses the switch for local *and* long distance features must use a "loop-around" trunk between the two software platforms. To avoid excessive post-dial delay and to allow the passing of Calling Party Number information, the loop-around trunk uses SS7 signaling rather than MF signaling.

Previously, SS7 loop-around trunks required two SMs (*intermodule* trunking, see Section 11.1). Therefore, loop-around trunks were not available on 5ESS[®]-2000 switch VCDX or single-SM 5ESS[®]-2000 switches, and these switches could not offer local and long distance features to a call that needed both types.

11.2.6 Feature Operation

The SS7 packet switching unit (PSU) supports single-SM-2000 loop-around *intramodule* trunks (intra-IMTs) by interfacing with the SS7 signaling network. This provides single-SM-2000 switches the capability of full interworking between local and toll software platforms, and allows a call originating on a line to access long distance platform (LDP) toll features such as the LDP Automatic Number Identification (ANI) table. The loop-around intramodule trunk configuration is illustrated in Figure 11.2-1 .

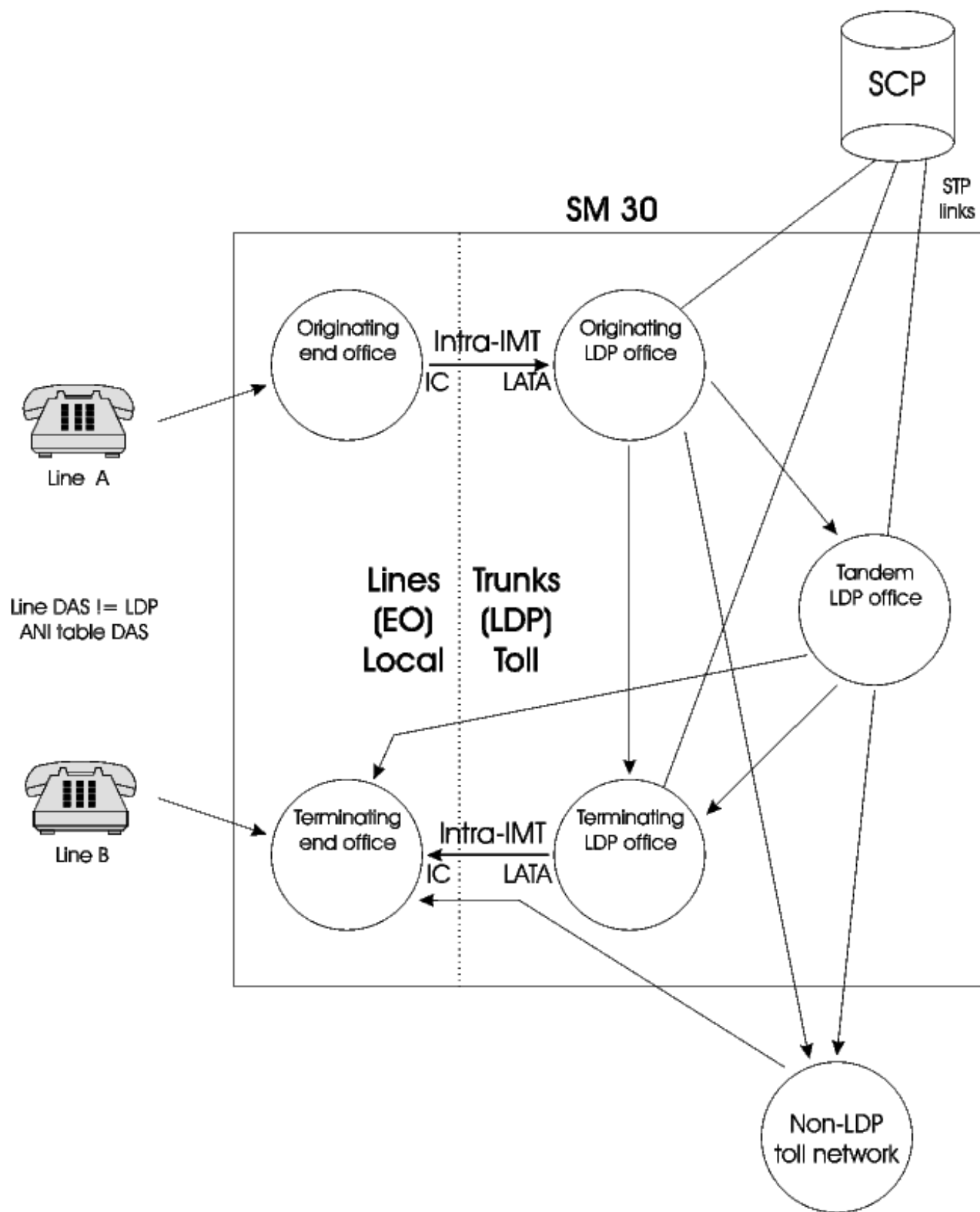


Figure 11.2-1 VCDX Loop-around Intramodule Trunk

Signaling messages for intramodule trunks don't leave the switch, but instead are intercepted in the message transport mechanism in the PSU and sent back to appropriate destinations in the software for processing as if they came from the external SS7 message network.

NOTE: The Intermodule Trunking feature (Section 11.1) refers to a two-SM loop-around trunk as an *intermodule* trunk, or IMT. The VCDX Loop-around Intramodule Trunk feature refers to a single-SM-2000 loop-around trunk as an *intramodule* trunk, or intra-IMT.

11.2.7 User Operation

11.2.7.1 For Subscribers

No subscriber actions are associated with this feature.

11.2.7.2 For Switch Personnel

Because the signaling messages are not sent out of the switch for intra-IMT trunk groups, a tester cannot use link monitor mechanisms to observe their contents. To observe the signalling content, use the CCS protocol monitor (see Section 8.2). A sample procedure follows.

- (1) SFID 260 must be active to use CCSPM.
- (2) Execute CCSPM for originating number:

```
exc:pmccs,isup,called=<dn>,hexdump
```

The `hexdump` option prints out raw data to the ROP.

OR

```
exc:pmccs,isup,called=<dn>,xlate
```

The `xlate` option stores the data in a readable format in an ASCII translation file (ATF) on the 3B20D/3B21D processor.

OR

```
exc:pmccs,isup,called=<dn>
```

Specifying no option defaults to the `xlate` option.

OR

```
exc:pmccs,isup,calling=8162205001;
```

where: Line A (calling number) is 816 220 5001 and Line B (called number) is 816 220 5002.

- (3) EXC:CCSPM input confirmation:

```
S4C0-43 99-03-03 08:42:51 000748 MAIPR N3 yBWM99-0003re
M exc:pmccs,isup,calling=8162205001; PF

S570-75 99-03-03 08:42:52 000749 SPM N3 yBWM99-0003re
M EXC PMCCS STARTED
  CALLING=8162205001 REPEAT=0
  SES=1 03/03 08:42:52 DUR=86400
  PROT=ISUP DIR=EITHER
```

```

XLATE    STATE=RECORDING

S570-75 99-03-03 08:42:56 000750 SPM N3 yBWM99-0003re
M EXC PMCCS PROCESSORS SCREENING
  SES=1 03/03 08:42:52

SM NUMBERS
  1      2      4    192

```

(4) Make one EO/LDP ISUP call (Line A to Line B): 10026 173131 05002

(5) EXC:CCSPM output confirmation:

```

S570-75 99-03-03 08:45:44 000762 SPM N3 yBWM99-0003re
M EXC PMCCS REPORTING - BEGINNING TRANSLATION
  CALLING=8162205001 TKGMN=988-0 REPEAT=0
  SES=1 03/03 08:42:52 03/03 08:45:45 DUR=86400
  PROT=ISUP DIR=EITHER
  XLATE 3 EVENTS RECORDED STATE=TRANSLATING
  ATF=/unixa/users/pmtran/atf.001

```

(6) The CCSPM output is on the 3B20D/3B21D processor in file /unixa/users/pmtran/atf.001

11.2.8 Engineering

11.2.8.1 Hardware Resources

No hardware considerations are associated with this feature.

11.2.8.2 Software Resources

No software considerations are associated with this feature.

11.2.8.3 Transition Considerations

No transition considerations are associated with this feature.

11.2.9 Interactions and Limitations

No interactions or limitations are associated with this feature.

11.2.10 Incompatibilities

No incompatibilities are associated with this feature.

11.2.11 Dependencies

No other features need to be installed or activated in order for this feature to work.

11.2.12 Isolation Constraints

No isolation constraints are associated with this feature.

11.2.13 Recent Change Provisioning

11.2.13.1 RC/V View 5.1 - Trunk Group

The intra-IMT must have its OPC populated with the OPC of the switch and its DPC populated in the DEST PT CODE field on RC/V View 5.1 in the format 000sss255 or 000255sss, where 000 is the network indicator for an intra-IMT, sss is the number of the switching module on which both ends of the loop-around trunk reside (1 through 192), and 255 indicates that the loop-around trunk is on a single SM-2000. Example: the 9-digit externally-defined DPC for an intra-IMT on SM 30 would be populated as:

TG	DPC	SM #	GPORT MODULE
1	000030255	030	Port number of one end of the intra-IMT trunk group member on SM 30
2	000255030	030	Port number of the opposite end of the intra-IMT trunk group member on SM 30

The INTER SM TRK field must be set to the value N to indicate that this is an intra-IMT (a single-SM loop-around trunk).

11.2.13.2 RC/V View 16.10 - Signaling Point Code

The intra-IMT must have a network indicator of 000 populated in the first three digits of the POINT CODE field on RC/V View 16.10.

Each DEST PT CODE value used on RC/V View 5.1 must first be entered on View 16.10.

11.2.14 Customer Premises Equipment (CPE)

Not applicable.

11.2.15 Maintenance Considerations

Not applicable.

11.2.16 Administration

11.2.16.1 Measurements

This feature does not impact measurements.

11.2.16.2 Billing

This feature does not impact billing.

11.3 CNI-BASED INTRAMODULE TRUNKING

11.3.1 Description

The ISUP Intramodule Loop-around Trunk feature, 99-5E-7213, implements single-SM loop-around trunks to offer local and long distance applications on a 5ESS[®]-2000 switch with a single SM-2000.

For PSU-based intramodule trunking, see Section 11.2 .

11.3.2 Availability

The ISUP Intramodule Loop-around Trunk feature is available in 5E13 and later software releases.

11.3.3 Environment

The ISUP Intramodule Loop-around Trunk feature is implemented on the 5ESS[®]-2000 switch and 5ESS[®]-2000 switch Compact Digital Exchange (CDX) switches equipped with SM-2000s.

This feature is designed primarily for switch configurations with only one SM-2000, but can be used with multiple-SM-2000 configurations.

11.3.4 Cross References

The following cross references apply to this feature:

- Feature Number: 99-5E-7213

11.3.5 Background

Because there is not full interworking between local and long distance software platforms (a call originating on a line cannot access the ANI table), a single call that uses the switch for local *and* long distance features must use a "loop-around" trunk between the two software platforms.

Previously, SS7 loop-around trunks required two SMs (*intermodule* trunking, see Section 11.1). Therefore, loop-around trunks were not available on single-SM 5ESS[®]-2000 switches, and these switches could not offer local and long distance features to a call that needed both types.

11.3.6 Feature Operation

The "single-SM loop-around trunk" is called an intramodule trunk or intra-IMT because only one switching module is involved. To avoid excessive post-dial delay and to allow the passing of the Calling Party and Charge Numbers and to preserve ISDN features, this loop-around trunk uses SS7 signaling rather than multifrequency (MF) signaling.

The intramodule loop-around trunk configuration is illustrated in Figure 11.3-1 .

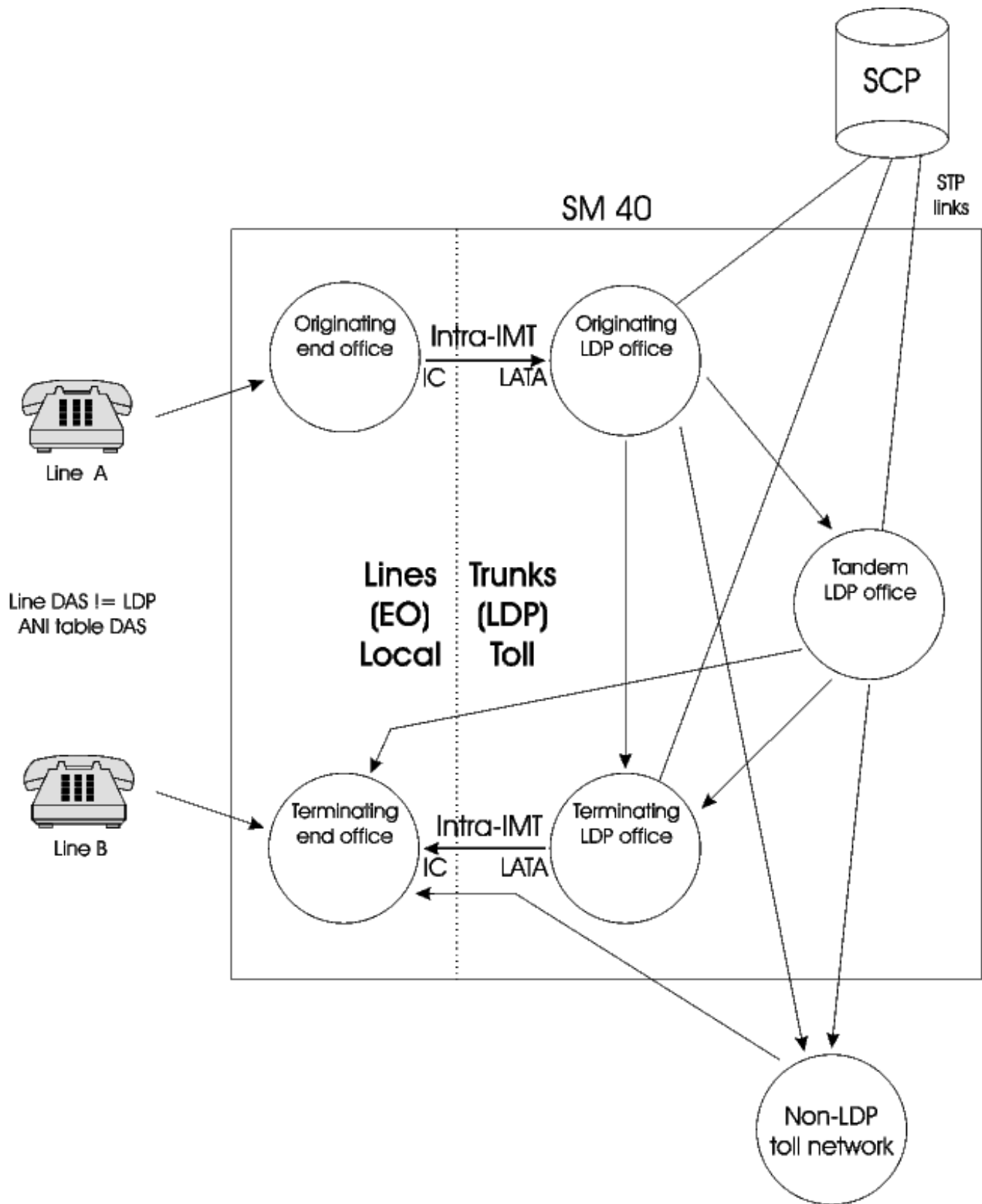


Figure 11.3-1 ISUP Intramodule Loop-around Trunk

Signaling messages for intra-IMTs don't leave the switch, but instead are intercepted and sent back to appropriate destinations in the software for processing as if they came from the external SS7 message network.

NOTE: The Intermodule Trunking feature (Section 11.1) refers to a two-SM loop-around trunk as an *intermodule* trunk, or IMT. The ISUP Intramodule Loop-around Trunk feature refers to a single-SM loop-around trunk as an *intramodule* trunk, or intra-IMT.

11.3.7 User Operation

11.3.7.1 For Subscribers

No subscriber actions are associated with this feature.

11.3.7.2 For Switch Personnel

Because the signaling messages are not sent out of the switch for intra-IMT trunk groups, a tester cannot use link monitor mechanisms to observe their contents. To observe the signalling content, use the CCS protocol monitor (see Section 8.2). A sample procedure follows.

(1) SFID 260 must be active to use CCSPM.

(2) Execute CCSPM for originating number:

```
exc:pmccs,isup,called=<dn>,hexdump
```

The `hexdump` option prints out raw data to the ROP.

OR

```
exc:pmccs,isup,called=<dn>,xlate
```

The `xlate` option stores the data in a readable format in an ASCII translation file (ATF) on the 3B20D/3B21D processor.

OR

```
exc:pmccs,isup,called=<dn>
```

Specifying no option defaults to the `xlate` option.

OR

```
exc:pmccs,isup,calling=8162205001;
```

where: Line A (calling number) is 816 220 5001 and Line B (called number) is 816 220 5002.

(3) EXC:CCSPM input confirmation:

```
S4C0-43 99-03-03 08:42:51 000748 MAIPR N3 yBWM99-0003re
M exc:pmccs,isup,calling=8162205001; PF
```

```
S570-75 99-03-03 08:42:52 000749 SPM N3 yBWM99-0003re
M EXC PMCCS STARTED
  CALLING=8162205001 REPEAT=0
  SES=1 03/03 08:42:52 DUR=86400
  PROT=ISUP DIR=EITHER
  XLATE STATE=RECORDING
```

```

S570-75 99-03-03 08:42:56 000750 SPM N3 yBWM99-0003re
M EXC PMCCS PROCESSORS SCREENING
SES=1 03/03 08:42:52

```

```

SM NUMBERS
1      2      4      192

```

(4) Make one EO/LDP ISUP call (Line A to Line B): 10026 173131 05002

(5) EXC:CCSPM output confirmation:

```

S570-75 99-03-03 08:45:44 000762 SPM N3 yBWM99-0003re
M EXC PMCCS REPORTING - BEGINNING TRANSLATION
CALLING=8162205001 TKGMN=988-0 REPEAT=0
SES=1 03/03 08:42:52 03/03 08:45:45 DUR=86400
PROT=ISUP DIR=EITHER
XLATE 3 EVENTS RECORDED STATE=TRANSLATING
ATF=/unixa/users/pmtran/atf.001

```

(6) The CCSPM output is on the 3B20D/3B21D processor in file /unixa/users/pmtran/atf.001

11.3.8 Engineering

11.3.8.1 Hardware Resources

No hardware considerations are associated with this feature.

11.3.8.2 Software Resources

No software considerations are associated with this feature.

11.3.8.3 Transition Considerations

No transition considerations are associated with this feature.

11.3.9 Interactions and Limitations

No interactions or limitations are associated with this feature.

11.3.10 Incompatibilities

No incompatibilities are associated with this feature.

11.3.11 Dependencies

No other features need to be installed or activated in order for this feature to work.

11.3.12 Isolation Constraints

No isolation constraints are associated with this feature.

11.3.13 Recent Change Provisioning

11.3.13.1 RC/V View 5.1 - Trunk Group

The intra-IMT must have its OPC populated with the OPC of the switch and its DPC populated in the DEST PT CODE field on RC/V View 5.1 in the format 000sss255 or 000255sss, where 000 is the network indicator for an intra-IMT, sss is the number of the switching module on which both ends of the loop-around trunk reside (1 through 192), and 255 indicates that the loop-around trunk is on a single SM-2000. Example: the 9-digit externally-defined DPC for an intra-IMT on SM 40 would be populated as:

TG	DPC	SM #	GPORT MODULE
1	000040255	040	Port number of one end of the intra-IMT trunk group member on SM 40
2	000255040	040	Port number of the opposite end of the intra-IMT trunk group member on SM 40

The INTER SM TRK field must be set to the value N to indicate that this is an intra-IMT (a single-SM loop-around trunk).

11.3.14 Customer Premises Equipment (CPE)

Not applicable.

11.3.15 Maintenance Considerations

Not applicable.

11.3.16 Administration

11.3.16.1 Measurements

This feature does not impact measurements.

11.3.16.2 Billing

This feature does not impact billing.

11.4 OSPS FEATURE GROUP D (FGD) CARRIER IDENTIFICATION CODE (CIC) EXPANSION

11.4.1 Description

The OSPS Feature Group D (FGD) Carrier Identification Code (CIC) Expansion feature allows the OSPS to interface with Feature Group D carriers when CIC codes are four digits in length. It also allows an OSPS to distinguish a Feature Group D carrier from a Feature Group B carrier that uses the same four-digit carrier code.

The OSPS Feature Group D (FGD) Carrier Identification Code (CIC) Expansion feature provides the capabilities to identify, route, and signal Feature Group D carrier calls with four-digit CICs.

With CIC expanding to four digits, several operation systems that interface with OSPS are impacted. This includes the Real Time Rating System (RTR), the Automated Charge Quotation System (ACQS), the Line Information Database (LIDB), the External Information System (EIS) and Automatic Message Accounting (AMA).

11.4.2 Availability

This feature is available in the 5E9(1) and later software releases.

11.4.3 TCAP CIC Expansion Indicator

In addition to the parameters contained in the LIDB TCAP query, the OSPS includes the new CIC Expansion Indicator parameter (TCAP CIC, which is found on Recent Change View 8.1). This parameter indicates to the LIDB that the OSPS can accept a four-digit CIC. This parameter is included only if the switch recent changeable parameter that determines whether the office will send or not send the TCAP CIC Expansion Indicator is set.

11.5 INTERSWITCH CALL FORWARDING

Interswitch Call Forwarding uses SS7 signaling to transport call history information. Signaling procedures for interswitch ISDN and non-ISDN call forwarding are supported. Interswitch Call Forwarding capabilities include:

- generating and updating the Original Called Number parameter, Redirecting Number parameter, and Redirection Information parameter on each forwarding of the call at the forwarding exchange.
- at a tandem exchange, passing the Original Called Number parameter, Redirecting Number parameter, and Redirection Number parameter.
- at the forwarding exchange, limiting the number of interswitch call forwardings to a maximum of ten. This includes procedures for incrementing the redirection counter field of the RI parameter on each forwarding (intraswitch or interswitch) and checking this counter before each interswitch forwarding is allowed.
- including optional parameters received (in the IAM for the incoming circuit) at the forwarding exchange in the outgoing IAM, with the exception of some parameters that are selectively discarded.

11.5.1 Optional ISUP Parameters

Optional ISUP parameters that may be present in an incoming IAM may be passed or reconstructed, updated, or discarded depending on the particular parameter and the type of call forwarding (CFBL/V/DA) active at the forwarding exchange. Any optional parameters that are not associated with call forwarding, but are currently received in an incoming IAM and passed by the current version of call forwarding (CFBL/V/DA), are included unchanged in the outgoing IAM. For details see "Treatment of Optional Parameters at the Forwarding Exchange," Section 11.5.5.2.

11.5.2 Checking The Forwarding Limit

The Stage 1 T1S1 description of non-ISDN call forwarding states that the maximum number of sequential forwardings is five. The Bellcore Technical Reference on ISDN call forwarding states that the maximum number of sequential call forwardings, intraswitch and interswitch is 10. To comply with Bellcore requirements, the redirection counter is incremented on every sequential forwarding, intraswitch or interswitch, and does not allow more than ten interswitch forwardings. This is the case regardless of the value of the internal call forwarding counter.

The switch supports an internal forwarding counter, which keeps track of intraswitch forwardings. The switch also supports an internal forwarding counter on a per-line basis that allows up to 32 call forwardings to a line.

The switch currently supports a "maximum number of forwardings" limit (CF_MAX). This limit is assigned per-call forwarding feature. As provided today, if the number of forwardings reaches the value stored in CF_MAX, the call is not forwarded again. CF_MAX currently has a default value of five. If the number of forwardings (both interswitch and intraswitch) exceeds ten, but has not exceeded CF_MAX, the call can continue to be forwarded within the switch up to CF_MAX, but cannot forward to another switch.

If the number of forwardings allowed by CF_MAX is reached, intraswitch in the switch, before the redirection counter reaches its limit of ten, the CF_MAX-imposed limit takes precedence and no more forwarding is allowed.

Providing this implementation solves two problems. The first allows the operating company to comply exactly with the Bellcore specification. The second problem which is resolved is backward compatibility. By allowing the operating company to set CF_MAX to some number higher than 10, the operation that their customers have today continues to be supported. For example, if some client currently allows calls to forward intraswitch for 30 times, the operating company can set CF_MAX to 30 and the call continues to forward up to 30 times provided the call does not forward off-switch.

11.5.3 Error Treatment

For the switch, the following procedures apply:

- (1) If the last attempted forwarding (the forwarding that takes the redirection counter over its specified limit) is due to CFBL (Call Forwarding Busy Line, or CFB) or CFV (Call Forwarding Variable, or CFU), (see the following for additional 1A *ESSTM* CFV error treatment), and if CFDA (CFNR) has not previously occurred on the same exchange, the call is cleared back to the calling party. For an SS7 interswitch call, a cause value of "user busy" is returned in the release message. The calling party hears busy tones.

If CFDA has previously occurred on the same exchange, the call is cleared back to the CFDA party. The CFDA user continues to receive alerting and the calling party continues to hear audible ringing.

- (2) If the last attempted forwarding is due to CFDA, the forwarding party continues to be alerted while the calling party continues to hear audible ringing.

11.5.4 First Call Forwarding

For the first forwarding (redirection) of the call, there are two parameters that are initialized: RI and OCN. The CdPN is recomputed (this is an existing capability). If the forwarding is to a number on another switch, these parameters are sent in an outgoing IAM. Even if the forwarding is to a number on the same switch, these parameters must still be initialized and updated. After the updates and additions, the following parameters are computed (that is, this information needs to be maintained/updated with each forwarding):

- Redirection information
- Original called number.

The added parameters are initialized as follows:

- Charge Number
 - Set the "O/E indicator" field to "even number of address signals." The CHN is to be a 10-digit number.
 - Set the "nature of address indicator" field to "ANI of the calling party; national number." The CHN is that of the forwarding party.
 - Set the "numbering plan" field to "ISDN numbering plan (CCITT Rec. E.164)."
 - Set the "address presentation restricted indicator" field as taken from the line data of the calling party.
 - Set the "address signal" octets to the digits of the calling (the forwarding) party.

- Redirection Information

For the first forwarding, the redirection information parameter is coded as follows:

- Set the "original redirection reason" field to the appropriate cause:

"unknown/not available"

"user busy"

"no reply"

"unconditional."

- Set the "redirection counter" field to "one" (0001).

NOTE: Although the VM system does not use this information, it is carried in the RI parameter and is used by call forwarding procedures.

- Set the "redirecting reason" field to the appropriate cause, which, for the first forwarding, is as the "original redirection reason."

- Original Called Number

Set the "address presentation restricted indicator" field as taken from the line data of the forwarding party.

- Called Party Number

Set the CdPN to the number that the call is to be forwarded to.

- Calling Party Number

Preserve the CPN.

11.5.5 Second Call Forwarding

For the second forwarding (redirection) of the call as determined by a redirection counter value equal to 1, there is one parameter that is initialized: the redirecting number. Two additional parameters are updated. They are the redirection information and the called party number parameters. After the updates and additions are made, the following parameters are computed (that is, this information needs to be maintained/updated with each forwarding):

- Redirection Information
- Redirecting Number
- Original Called Party.

The parameter updates are as follows:

- Charge Number

Set the "address signal" (address digits) octets to the digits of the forwarding party. The CHN presentation restriction setting is taken from the line data of the forwarding party. Set all other fields as for the first forwarding.

- Redirection Information

For the second forwarding, the redirection information parameter is coded as follows:

- Preserve the "original redirection reason" field.
- Increment the "redirection counter" field by one.
- Set the "redirecting reason" field to the appropriate cause, which may be different for each hop.

"Unknown/not available"

"User busy"

"No reply"

"Unconditional."

- Redirecting Number

For the second forwarding, the redirecting number parameter is coded as follows:

Set the "numbering plan" field to "ISDN numbering plan (CCITT Rec. E.164)" (001).

The "nature of address" field, odd/even indicator, and address signal field is populated based on the line data of the forwarding party.

- Original Called Number

Preserve the OCN through multiple forwardings.

- Called Party Number

Set the CdPN as specified earlier for the first forwarding.

- Calling Party Number

Preserve the CPN through multiple forwardings.

11.5.5.1 Third or Greater Call Forwarding

For the third or greater forwarding (redirection) of the call as determined by a redirection counter value equal to 2 or greater, there are three parameters that are updated: the RI, the RgN, and the CdPN.

For the switch, the maximum number of intraswitch call forwardings is recent changeable and has a maximum value of 32. After the updates are made, the following parameters are computed (that is, this information needs to be maintained/updated with each forwarding).

- Redirection Information
- Redirecting Number
- Original Called Party.

The parameter updates follow the same procedures required for the second forwarding described earlier.

The Interswitch Voice Messaging feature (ISVM) uses a subset of SS7 procedures for interswitch signaling call forwarding. For more information, refer to "Interswitch Voice Messaging Service," Section 11.14.

11.5.5.2 Treatment of Optional Parameters at the Forwarding Exchange

After an initial address message (IAM) is received, once the exchange determines that a call is forwarded, the forwarding limit is checked and parameters essential to the forwarded call are set for inclusion in the IAM for the outgoing circuit as described in Section 11.5. Treatment of optional parameters in the IAM other than the calling party number (CPN) parameter, redirection information (RI) parameter, original called number (OCN) and the redirecting number (RgN) parameter is specified here.

All optional parameters received by the forwarding exchange in the IAM for the incoming circuit is included in the outgoing IAM coded as received, except for the following parameters which require additional processing.

(a) Access Transport Parameter (ATP)

If the forwarding party is non-ISDN, the forwarding exchange discards the ATP. The ATP is not included in the outgoing IAM for all types of call forwarding, [that is, call forwarding unconditional (CFU), call forwarding busy (CFB), and call forwarding no reply (CFNR)].

If the forwarding party is ISDN, the forwarding exchange examines the contents of the ATP if received in the IAM. If the ATP contains a Q.931 called party subaddress information element or a redirecting subaddress information element, the information element(s) is discarded. All other information received in the ATP is included in the ATP in the outgoing IAM, for all types of call forwarding for intra-LATA calls. Inclusion of the ATP in the outgoing IAM for inter-LATA calls is subject to interexchange carrier (IEC) subscription.

(b) Charge Number (CHN)

The CHN parameter received in the incoming IAM is **not** forwarded. The switch may generate a new CHN parameter for inclusion in the outgoing IAM. The conditions under which a CHN parameter is generated follows the procedures for an originating exchange.

(c) Generic Address Parameter (GAP)

If the forwarding party is non-ISDN, GAP, with type of address field set to "Supplemental User Provided Calling Address - not screened" or "Supplemental User Provided Calling Address - failed network screening," is not forwarded. Generic Address parameters with type of address field not set to "Supplemental User Provided Calling Address - not screened" or "Supplemental User Provided Calling Address - failed network screening" is treated as unrecognized optional parameters as described in item (g).

If the forwarding party is ISDN, GAP, with Type of Address field set to "Supplemental User Provided Calling Address - not screened (0000 0011)" or "Supplemental User Provided Calling Address - failed network screening (0000 0010)," follows the requirements in Section 11.5 for the Calling Party Number (CPN) parameter at the forwarding exchange. GAP, with type of address field not set to "Supplemental User Provided Calling Address - not screened (0000 0011)" or "Supplemental User Provided Calling Address - failed network screening (0000 0010)," is treated as unrecognized optional parameters as described in item (g).

(d) Originating Line Information (OLI)

Regardless of the type of call forwarding or whether the forwarding party is ISDN, the OLI parameter, if received in the incoming IAM, is discarded at the forwarding exchange. If the forwarded leg of the call is an internetwork call, the OLI parameter may be generated for inclusion in the outgoing IAM.

(e) Transit Network Selection (TNS)

The procedures specified for the OLI parameter in "Treatment of Optional Parameters at the Forwarding Exchange," Section 11.5.5.2 also apply to the TNS parameter. It is noted, however, that receipt of the TNS parameter at the forwarding exchange is not expected.

(f) User-to-User Information (UUI)

If the forwarding party is non-ISDN, the forwarding exchange discards the UUI. The UUI is not included in the outgoing IAM for all types of call forwarding, [that is, call forwarding unconditional (CFU), call forwarding busy (CFB), and call forwarding no reply (CFNR)].

If the forwarding party is ISDN, UUI is not discarded at the forwarding exchange for intra-LATA calls. The

inclusion of the UUI parameter in the outgoing IAM for inter-LATA calls is subject to the IEC subscription to receive UUI.

(g) Unrecognized Optional Parameters

Unrecognized optional parameters received by the forwarding exchange in the IAM is included in the outgoing IAM coded as received.

11.6 ISUP MEASUREMENTS PROTOCOL

11.6.1 DLN-AM Queues

The DLN-AM queues in the AM are identified by a new processor code for the DLN. CCS processes in the SM address all CCS signaling messages to the new DLN-AM queues using the DLN processor code recognized by the MCSU. This processor code is supplied to the SM at initialization in offices equipped with the DLN.

The data stream linking a CM with a DLN flows through AM main memory. One segment is required for each bidirectional stream. Since both CM sides are active, two segments are required. The segments are identical and are "owned" by the RINGMON kernel process. They are shared by the Message Switch Kernel Process (MSKP).

The segment is variable in size from a minimum of 1 page to a maximum of 64 pages, with a page containing 2048 bytes. This allows per office engineering for various stream capacities. The segment contains a buffer for each stream direction. These buffers may be different sizes in each direction. These segments are shared between the RINGMON and MSKP processes only, no other process is affected.

The buffer structure provides for optimal transfer of data without being aware of the data content. Data for either side of the stream is loaded in block mode. A block contains an integral number of messages. The MCSU handles messages individually, so its block consists of exactly one message. The DLN will handle blocks containing a variable number of complete messages. The buffer can also be unloaded in a block mode, where a block is a variable number of messages. Loading and unloading in DMA block mode is the most efficient method of accessing memory.

The buffer scheme provides a smooth transition from the bottom to the top at the wrap around point. A block of data does not have to be split when transitioning from the bottom to the top. Typically, circular buffers wrap from the buffer bottom to the top by having to break a message into two parts. This adds complexity to buffer loading software and causes more buffer transfers than is necessary.

The buffer structure contains the three following contiguous components:

- A header containing administrative fields.
- An incoming buffer as viewed from the CM.
- An outgoing buffer as viewed from the CM.

11.6.2 30-Minute Traffic Report

Many of the ISUP measurements are supported in the switch and appear on the hourly report. However, since the ISUP counts are merged with other CCS protocol counts, the ISUP users requested that a separate report be generated every 30 minutes.

The 30-minute traffic report contains the ISUP measurements that were a part of the hourly report, plus some new measurements requested by the users. For more information on measurements, refer to the 235-070-100, *Traffic and Plant Measurements* document.

Following is a list of required 30-minute measurements:

- Total ISUP messages sent.
- Total ISUP messages received.

- Unreasonable messages received - (This means that the switch received a known message in a call state when it does not expect such a message.)
- Release initiated due to abnormal conditions - An outgoing ISUP process which sends an **IAM** or **CRM** message and receives/encounters one of the following events before receiving an **ACM** (or an early **ANM** before **ACM**) will peg the count of unsuccessful ISUP attempts.
 - RSC
 - UCIC
 - COT Failure
 - Unexpected Message
 - ACM Timeout
 - CRA Timeout
 - BLO
 - REL w/any cause

This count will not be pegged for forward **REL** messages.

- Circuit blocked - (A **BLO** message was received on an in-service trunk.)
- Termination failure due to glare - (The terminating terminal process encountered glare, backed out of the route request, and initiated a rehunt to another circuit.)
- Continuity failure - (The terminating terminal process attempts to run a continuity test that failed.)
- Initiation of a trunk rehunt for any other reason other than glare or continuity test failure.
- Total unsuccessful attempts - (This means that the terminating terminal process has failed to complete the ISUP call for any reason.)

The following conditions are counted at the controlling switch (the forward-most switch in the sequence handling the call when the problem occurs). An **REL** message is sent to earlier switches in the call chain and counts are tallied only at the controlling switch.

- Switching congestion - (The switch has failed the call due to congestion overload.)
- No circuit available - (The routing and terminal allocation subsystem sends a message to the originating terminal processor that no circuit is available for the call.)
- Address incomplete - (The switch attempts to analyze the called number in the incoming IAM and is unable to interpret it.)
- Temporary failure - (Call has failed in this switch due to temporary failure.)
- Unlocated number - (The switch tried to locate the called number in the listed directory number translations and could not find it.)
- Busy - (The called number is busy and does not have call waiting or does not respond to the beep.)

- Destination out of service - (The switch completes the trunk hunt, attempts to terminate at the chosen port, and tries to send the IAM message. However, the data port circuit of the far-end switch is out of service and no alternate destination switch is available.)
- Other causes - (The call has failed, but the reason is not defined in the items listed previously. This is a default cause.)

The associated input/output messages are supported for all 30-minute traffic reports.

All 30-minute measurements appear in one section, grouped into four subsections based on the nature of the measurement count. Summarizing the 30-minute measurement requirements, Tables 11.6-1, 11.6-2, 11.6-3 and 11.6-4 give the 30-minute traffic report usage, performance, circuit availability, and end-to-end connection performance.

Table 11.6-1 30-Minute Traffic Report: ISUP Utilization

REPORT EVENTS	30-MN REPT	1-HR REPT	COUNT LOCATION	CAUSE VALUE	SUB-SYS.
Total ISUP Msgs. Sent	Yes	No	All Switches	N/A	CCS
Total ISUP Msgs. Recvd.	Yes	No	All Switches	N/A	CCS

Table 11.6-2 30-Minute Report: ISUP Performance

REPORT EVENTS	30-MN REPT	1-HR REPT	COUNT LOCATION	CAUSE VALUE	SUB-SYS.
Unreasonable Msgs. Recvd. (& MDII)	Yes	Yes	At Switch Where Event Occurs	N/A	CCS
REL Initiated (Abnormal Conditions)	Yes	No	All Switches (Both Directions (& MDII))	N/A	CCS

Table 11.6-3 30-Minute Traffic Report: ISUP Circuit Availability

REPORT EVENTS	30-MN REPT	1-HR REPT	COUNT LOCATION	CAUSE VALUE	SUB-SYS
Circuit Blocked	Yes	No	At Switch Where Event Occurs (& MDII)	N/A	TM
Termination Failure Due to Glare	Yes	No	At Switch Where Event Occurs	N/A	CCS
COT Failure	Yes	Yes	At Switch Where Event Occurs (When COT Failure Occurs)	N/A	CCS
Initiate Trunk Rehunt For Any Other Reason	Yes	No	At Switch Where Event Occurs	N/A	CCS

Table 11.6-4 30-Minute Traffic Report: ISUP End-to-End Connection Performance

REPORT EVENTS	30-MN REPT	1-HR REPT	COUNT LOCATION	CAUSE VALUE	SUB-SYS
Total Unsuccessful Attempts	Yes	No	All Switches (Count Until ADC Rec.)	N/A	CCS
Switching Congestion	Yes	No	At Switch where Event Occurs (& MDII)	42	CCS

No Circuit Available	Yes	No	At Switch Where Event Occurs (& MDII)	34	CCS
Address Incomplete	Yes	Yes	At Switch Where Event Occurs (& MDII)	28	CCS
Temporary Failure	Yes	No	At Switch Where Event Occurs (& MDII)	41	CCS
Unallocated Number	Yes	Yes	At Switch Where Event Occurs (& MDII)	1	CCS
Busy	Yes	No	At Switch Where Event Occurs (& MDII)	17	CCS
Destination Out of Service	Yes	No	At Switch Where Event Occurs (& MDII)	27	CCS
Other Causes	Yes	No	At Switch Where Event Occurs (& MDII)	a	CCS
Notes:					
a. Default Cause Value.					

11.6.3 24-Hour Plant Measurement Report

The following items are counted for each interexchange carrier or international carrier and reported on a per-office basis in the 24-hour plant measurement report.

Item	Comments
COT failure	COT failures after two attempts (at end office and access tandem)
Total incoming MDIIs	For SS7 circuit groups directly connected to an IEC (at end office and access tandem)
Total outgoing MDIIs	For SS7 circuit groups directly connected to an IEC (at end office and access tandem)

Other plant measurements included on the 24-hour report are the expiration of the timer for toll call record assembler (TCRA) and the total incoming and outgoing MDIs for each SS7 circuit group.

Only 20 trunk groups can be selected and reported at one time. The following is an explanation of these items:

Item	Comments
TCA	Due to expiration of the timer at a gateway toll office for SS7 circuit groups connected to an LEC access tandem.
Total Incoming MDIIs	For SS7 circuit groups connected to an LEC end office or access tandem (at a gateway toll office).
Total Outgoing MDIIs	For SS7 circuit groups connected to an LEC end office or access tandem (at a gateway toll office).

11.7 ADVANCED SERVICES PLATFORM (ASP)

The Advanced Services Platform provides a set of service-independent network capabilities within the switch that can be used with feature logic within the SCP to provide new features. The Advanced Services Platform feature supports a network architecture that encompasses both digital and key analog switches to provide good service area coverage while limiting the investment required in embedded base systems. The ASP capabilities are based on accepted industry standards. Switching equipment and other key architectural components meeting these standards are available from Lucent Technologies as well as other vendors.

ASP supports two levels of functionality. The first is the service switching point (SSP) with complete ASP feature capabilities resident in the switch. The second is the network access point (NAP) which equips a switch with a limited subset of ASP functionality. In particular, the NAP does not communicate with an SCP. Instead, it routes ASP calls to an SSP for processing.

NOTE: The 5ESS[®]-2000 switch can no longer be configured as an NAP.

The ASP provides a platform of service-independent capabilities at a switch that allows it to interact with an external element, a service control point (SCP), via Signaling System 7 (SS7) Transaction Capability Application Part (TCAP) messages to help determine appropriate call handling treatment.

The NAP can recognize trigger events, like an SSP, but rather than launch a query to an SCP, it uses Feature Group D (FGD) or SS7 signaling to route the call to an SSP which, in turn, conducts the dialogue with the SCP.

Triggering occurs in both the NAP and the SSP. It is the process by which the switch determines that a query must be made to the SCP database.

Querying is the process of assembling an SS7 Transaction Capabilities Application Part (TCAP) message and launching the query across the SS7 network. The content of the query is determined by the type of trigger encountered by the switch.

After launching a query to the SCP, the SSP will await further instructions from the SCP. Common responses received from the SCP include routing and billing instructions, terminating announcement or interactive announcements (in which the caller is prompted for information).

ASP release 0.1B features are available on the 5ESS[®]-2000 switch Very Compact Digital Exchange (VCDX) in a 5E11 software update; release 0 is not available on a VCDX. For a description of the ASP capabilities available in the VCDX environment, or for further information regarding ASP in general, refer to the following documents:

- 235-190-125, *Advanced Services Platform Release 0 and Release 0.1A Feature Document*
- 235-190-126, *Advanced Services Platform Release 0.1B Feature Document*
- 235-030-100, *Advanced Services Platform Network Architecture and Service Consideration Guide*

The Local Number Portability (LNP) service, which is a capability supported by ASP, is also available on the VCDX in a 5E11 software update, and on the 5ESS[®]-2000 switch beginning in the 5E12 software release. Refer to one of the following documents for details:

- 235-190-127, *Number Portability User's Guide*
- 781-610-300, *Number Portability Roadmap*

11.8 SERVICE SWITCHING POINT 800 (SSP800) NUMBER SERVICE FEATURE

11.8.1 Description

11.8.1.1 Service Switching

The Service Switching Point (SSP) feature enables the switch to interface with telephone company databases for implementing "number services," such as the 800 service. This section deals specifically with 800 number service. The switch with this feature can be an end office, tandem office, or access tandem.

NOTE: The 800 Service is not limited to the 800 NPA if the switch has implemented a toll-free treatment feature which allows additional toll-free Service Access Codes (SAC) such as 888 or 877.

The interface to the service control point (SCP) database is provided by Signaling System 7 - Transaction Capabilities Application Part (SS7 TCAP). Number services like the 800 service require special numbers to be dialed and require special call handling. The switch provides for routing 800 number service calls directly from the equal access end office or access tandem switch within the local access transport area (LATA) or to IEC. The reply from the SCP database provides information for routing the call.

The number service calls are originated by a customer dialing a directory number with a special numbering plan area. All 800 number service calls dialed with 10XXX prefix are blocked. Originations with a 0+ prefix are blocked at the option of the end office.

Dialing may be from an end office station, from a co-located station at a tandem, or access tandem office. Therefore, number service calls are identified on both line and trunk originations. If the call originates at an end office equipped with SSP capability, the SSP processing takes place at that time. Calls originating from an end office not equipped with SSP are routed to a switch (within the same LATA) having SSP capability. The SSP800 service is blocked for circuit-switched data calls.

11.8.1.2 Access Tandem Office

11.8.1.2.1 Access Tandem Function

Access tandem offices are able to receive calls from lines co-located at the office or from end offices which have already identified the call as a toll-free SAC number needing processing by another switch. End offices that may direct toll-free SAC number service calls to the access tandem are as follows:

- Equal access end office
- Non-equal access end offices using traditional signaling
- Non-equal access end offices using CAMA signaling
- Tandem offices.

Regardless of the type of originating office, the access tandem should be able to identify the LATA of the office by the incoming trunk group. Offices forwarding calls to an access tandem switch must ensure that all calls on a given trunk group are from the same LATA. It may be necessary to have several trunk groups to the access tandem meet this requirement. Although an access tandem may perform the tandem function for more than one LATA, calls between LATAs are forwarded to IECs for completion.

The access tandem must be able to construct partial automatic number identification (ANI) where a full ANI is not available. Either a 3-digit ANI (NPA) or a 6-digit ANI (NPA-XXX) is used for queries to the SCP database and automatic message accounting (AMA). Only a 3-digit ANI is used for calls handed off to IECs when 10 digits are not

available. The SCP database may return a translated plain old telephone service (POTS) number, or an untranslated toll-free SAC number to be routed. The ANI information used for outpulsing translated calls is "24."

11.8.1.2.2 Calls from Equal Access End Offices

Signaling: The sequence, KP+0ZZ+XXX+ST is received from an equal access end office. For POTS calls, a path is immediately cut through to the carrier specified by the XXX in the sequence. For SSP calls, since the real carrier is not yet known, a wink is returned to the equal access end office to initiate a second stage outpulsing. The equal access ANI sequence, KP+II+3/10D+ST consisting of all ten calling party digits, if known, is then sent to the access tandem. The last sequence received is the called number in the form KP+NPA+NXX+XXXX+ST. The access tandem returns an acknowledgment wink to the equal access end office. After the query is sent to the SCP database and a response is received, the received digits are then outpulsed to the far-end office. The "handshaking" that takes place in this procedure is shown in Figure 11.8-1 .

Number Service Identifier: The pseudo-carrier received in the first stage signaling identifies the number services and the toll-free Service Access Code (SAC) digits (such as 800 or 888) identify toll-free SAC number services.

ANI Handling: If only the 3-digit NPA is received, this is used to query the SCP database. If both the NPA and NXX of the calling party are known, the 6 digits are used to query the SCP database. The ANI "24" is used for translated POTS calls; otherwise, the "II" code digits received are outpulsed.

11.8.1.2.3 Calls from End Offices Using Traditional Signaling

Signaling: The called number sequence, KP+NPA+NXX+XXXX+ST, is received first, when originating in a non-equal access end office. The call sequence for calls from offices with traditional signaling is shown in Figure 11.8-2 .

Number Services Determination: The access tandem identifies the number service calls from the 3- or 6-digit translation of the called number. A special 00Y code may replace the NPA of the called number to communicate additional information from the end office to the access tandem. The 00Y code may communicate originator NPA, LATA, and coin originators.

ANI Handling: The ANI is not received by an end office using traditional signaling. The ANI is constructed using the NPA based on the incoming trunk group. The II information digits indicate whether the origination is from a coin line. If a 00Y code is received in place of the NPA of the called party, the constructed NPA is used for outpulsing to the far-end office. If a translated POTS number is routed, the II digits are 24. Table 11.8-1 contains a mapping of "II" codes for traditional signaling calls and non-translated toll-free Service Access Code (SAC) numbers.

Table 11.8-1 Traditional Signaling "II" Code Meanings

CONDITION	II
Coin Line	27
No Coin Line	00
Undeterminable	23

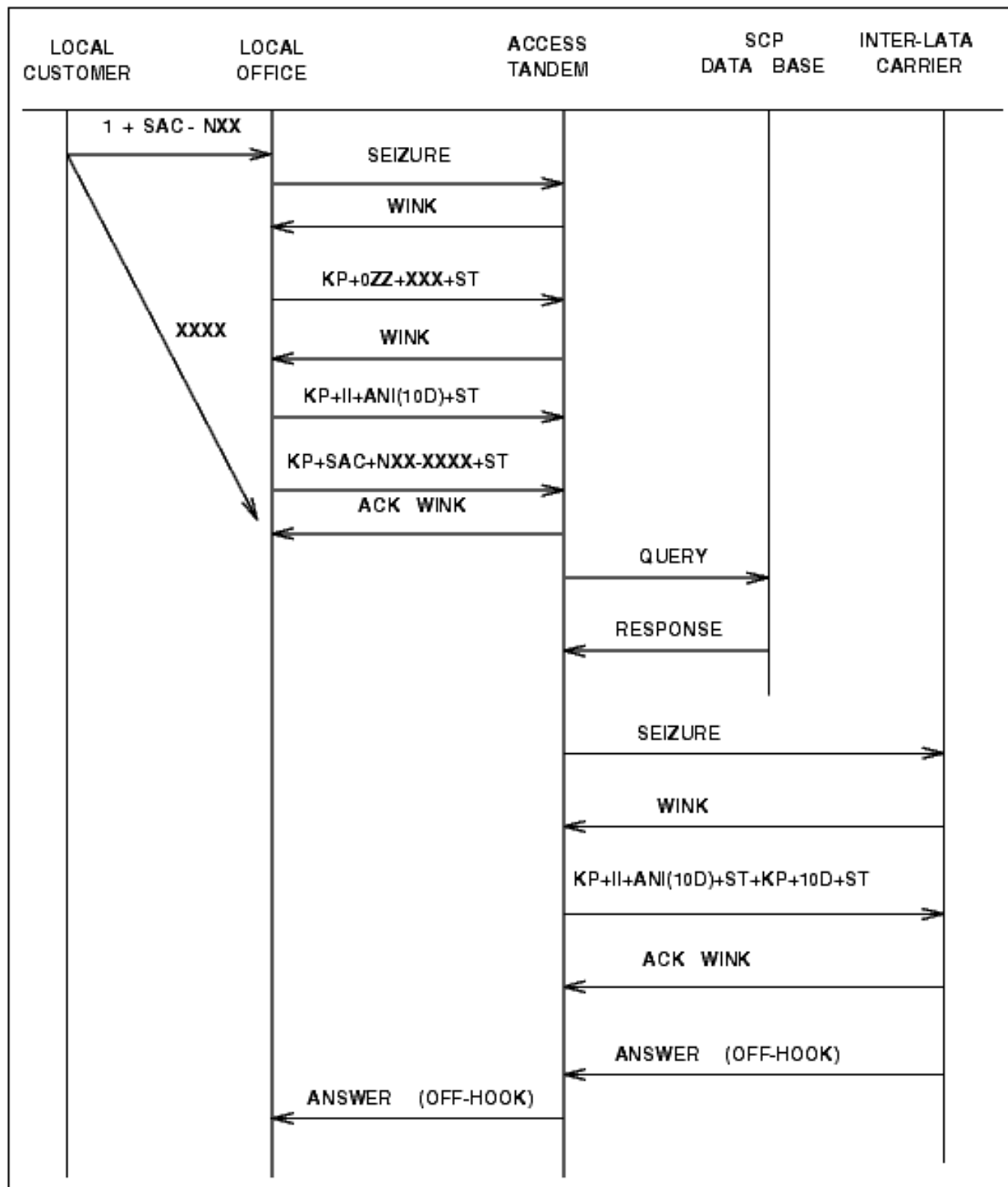


Figure 11.8-1 Equal Access Signaling Sequence

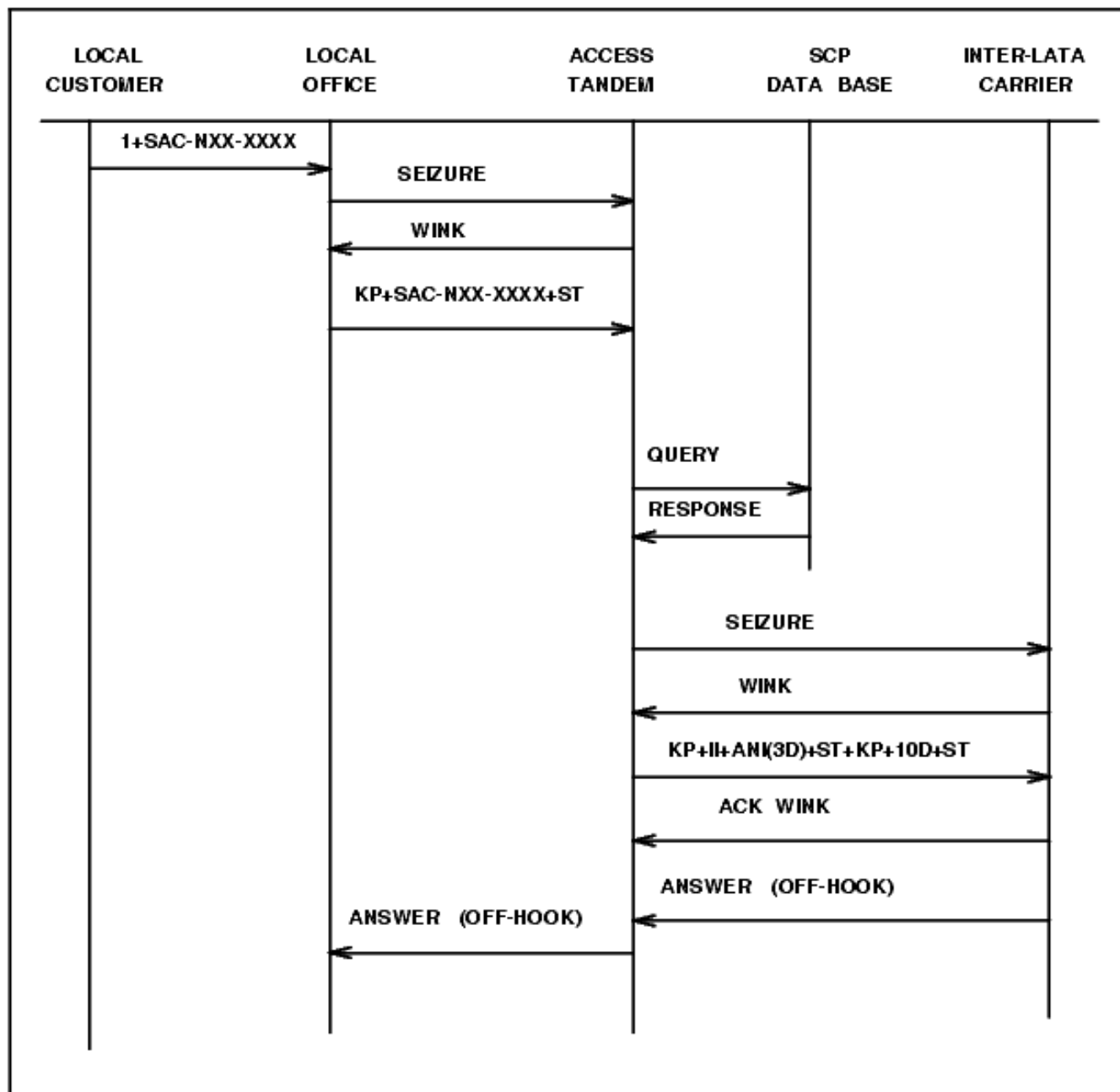


Figure 11.8-2 Traditional Signaling Sequence

11.8.1.2.4 Calls from an End Office Using CAMA Signaling

Signaling: Just as calls from a non-equal access end office, the called number sequence, KP+NPA+NXX+XXXX+ST, is received first. The access tandem returns a steady off-hook after receiving the called number sequence. The end office interprets the off-hook as a request to send an ANI to the access tandem. The CAMA ANI sequence, KP+I+7D+ST, consists of the 7-digit calling party. A representation of the signaling sequence is shown in Figure 11.8-3.

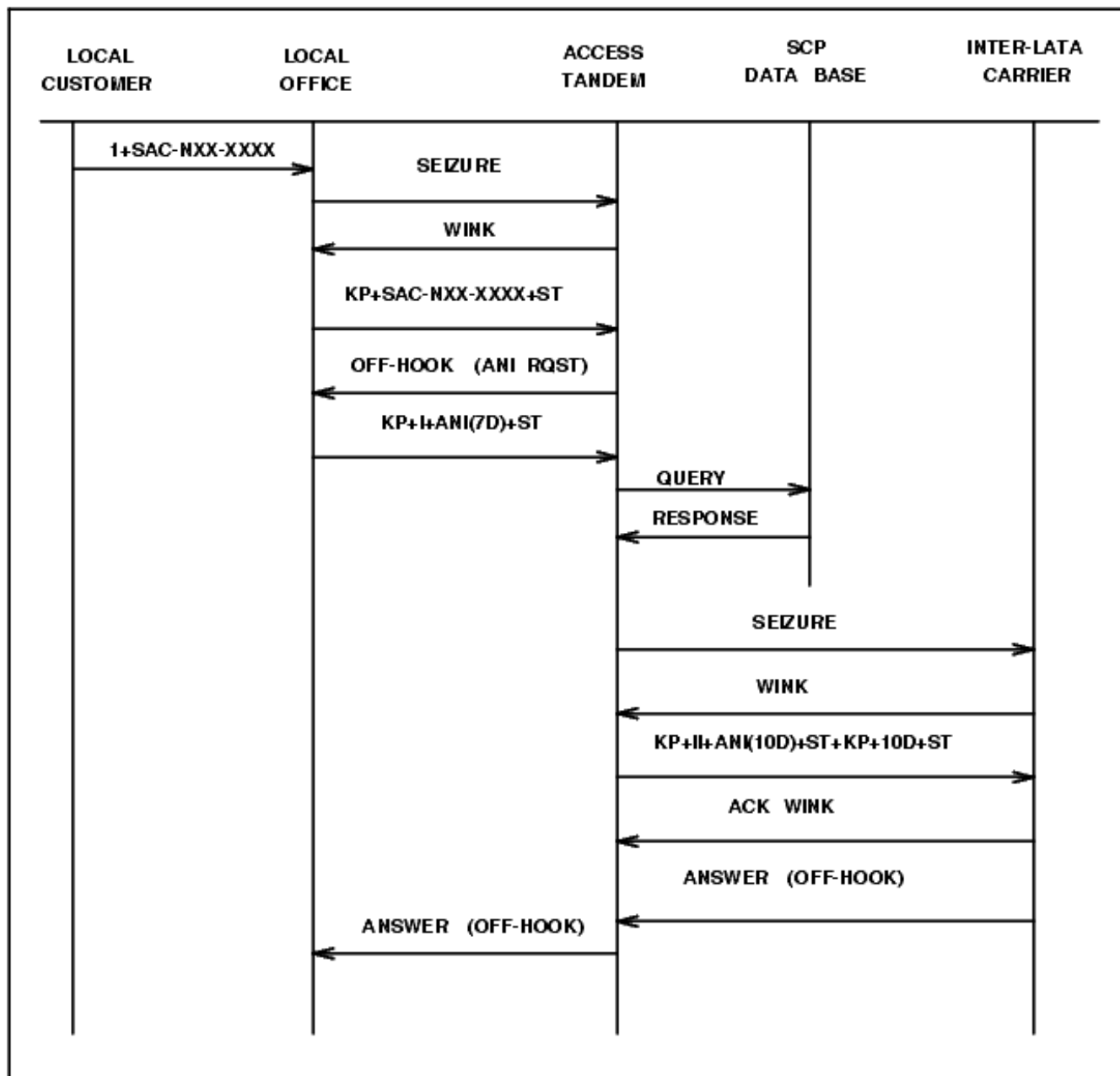


Figure 11.8-3 CAMA Signaling Sequence Cama signaling sequence

Number Services Determination: The access tandem must identify number services calls based on the 3- or 6-digit translation of the called number. Calls from coin stations, or any other situation where an ANI is not available require a special 00Y code to replace the NPA of the called number. The 00Y may indicate originators NPA, LATA, and coin indication.

ANI Handling: The NPA is determined from the 00Y code or by the incoming trunk group. The single "I" information digit is converted to a 2-digit "II" for further handling. If a translated POTS number is routed, the "II" digits are 24. If the origination is from a coin station, the "II" digits are set to 27. If the numbers are non-translated, use Table 11.8-2

Table 11.8-2 Mapping Conversion of "I" Codes to "II" Codes

I	II	MEANING
0	23	Noncoin/Coin Don't Know
1	01	Multiparty
2	23	ANI Failure
3	23	Noncoin POTS Observed
4	01	Multiparty Observed
5	23	ANI Failure Observed
6	06	Hotel
7	07	Coinless etc.

If the 00Y code is received in place of the called party NPA, the constructed NPA is outpulsed to the far-end office.

Calls From Tandem Offices: The access tandem may receive calls from a local tandem office. The ANI is received from these offices and is treated similar to the non-equal access end office.

11.8.1.3 Tandem Office

Offices serving as tandem offices to a nearby non-equal access end office may be equipped with the SSP capability, and meet all the requirements of an access tandem.

11.8.1.4 Equal Access End Office

Some equal access end offices have SSP capability. The number service is identified by the toll-free Service Access Code (SAC) of the dialed digits (such as 800 or 888). The query is sent to the SCP database just as explained for the access tandem.

11.8.2 Availability

The SSP feature for toll-free Service Access Code (SAC) service, such as 800 or 888 numbers is available with the switch, 5E7 and later software releases.

11.8.3 Implementation

11.8.3.1 Feature Assignment

The SSP function may be assigned to an equal access end office (EAEO), an access tandem, or a tandem office. The difference between the access tandem SSP and a tandem/SSP is a tandem SSP does not have direct trunks to an IEC. However, both offices must handle outgoing equal access signaling to a carrier.

11.8.3.2 Maintenance

No new office maintenance requirements are imposed by SSP capability. Infrequent recent changes on trunk groups may be necessary to maintain consistency with changes in the LATA or NPA boundaries. The performance of the SSP capability is observed from various measurements in the office and as a part of the CCS network.

11.8.3.3 Reliability

All SSP failure encounters appear on traffic and network maintenance reports. Failures across signaling link interfaces can be traced using existing routing and translation tests.

If the switch receives invalid data in a message from the database, an error message is sent to the database. If the billing data is invalid, the call is completed and the error message report is sent to SCP data base if a terminating message is requested by the SCP.

11.8.4 Feature Operation

11.8.4.1 TCAP Operation

The TCAP process assists service features such as the number service features (like the 800 Service feature). In a number service feature, the digits dialed by the user influence how the call is handled. In the 800 Service feature, a query is sent to the SCP using TCAP messages. Instructions are returned to the 800 Service feature which then invokes the TCAP to analyze the message.

NOTE: The 800 Service is not limited to the 800 NPA if the switch has implemented a toll-free treatment feature which allows additional toll-free Service Access Codes (SAC) such as 888 or 877.

11.8.4.2 Network Management

The network management subsystem contains the automatic call gap (ACG) control tables and the necessary support functions to maintain them. These ACG tables store information, received in query responses, relating to how to throttle query traffic to the SCP. The switch uses a maximum of 80 controls. The ACG component is contained in the response message sent to the SSP for queries relating to a problem. The SSP then adjusts further queries to the database as indicated by the control gap interval and duration level in the ACG message.

Control installation and application are performed in the administrative module (AM) or the direct link node (DLN), depending on the CNI configuration. Controls are installed and removed as directed by the response from the SCP database. Code control applications are performed before the query is sent to the SCP database.

Network management counts and discrete messages are used to report measurements to the EADAS and ON-SITE systems, as requested. The ACG component indicates that an ACG control should be installed in the switch on the 6- or 10-digit number returned in the message. This number is always either the NPA-NXX or NPA-NXX-XXX of the original dialed number sent in the initial query.

NOTE: There is no way to examine the ACG and controls cannot be manually installed. These are all internal functions.

11.8.4.3 Automatic Message Accounting

When a toll-free Service Access Code (SAC) service call (such as 800 or 888 call) is dialed at an SSP office, the AMA record for access charge billing, and possibly end-user billing, is made at the SSP, using the standard AMA format. The access charge billing record is made where access to the carrier is obtained, either in the access tandem SSP or the equal access end office SSP. The record made at the access tandem SSP is used for billing purposes. However, during transition, when only a subset of toll-free SAC calls are treated as number service calls, the record made at the end office or the CAMA office is used.

Ten new structure codes are required to support billing for toll-free SAC and other number service billing (see Table 11.8-3).

Table 11.8-3 Call Codes for Number Service Billing

STRUCTURE CODE	INTEREXCHANGE CARRIER CONDITIONS
00360	Number Service
00361	Number Service - Alternate Billing Number
00362	Number Service - Long-Duration
00363	Number Service - Long-Duration Alternate Billing Number
STRUCTURE CODE	TELEPHONE COMPANY CONDITIONS
00364	Number Service
00365	Number Service - Alternate Billing Number
00366	Number Service - Long-Duration
00367	Number Service - Long-Duration Alternate Billing Number
00368	Number Service - Unanswered
00369	Number Service - Unanswered Alternate Billing Number

Special number service structure code population is described as follows:

- (1) **The LATA Field:** This field consists of four characters. The first three define the LATA from which the call originated. The fourth character is a sign character.
- (2) **The Customer's Revenue Accounting Office Number Field:** This field consists of four characters. The first three characters contain the customer's 3-digit revenue accounting office. The fourth character is a sign character. If the customer's revenue accounting office is not available, the code contains zeros.
- (3) **The Alternate Billing Number Field:** This field consists of 12 characters. The first character is zero, the next ten characters are the ten digits of the billing number, and the last character is a sign character. The billing number is obtained from the SCP database optional billing number field. If an alternate billing number is not available, a structure code not containing an alternate billing number field is used.
- (4) **The Destination Overseas Indicator, Destination NPA, and Destination Number:** These are obtained from the SCP database routing number. The routing number may be the POTS number to which the call is to be routed or the number service number that the calling party dialed. If it is the number service number dialed, the dialed number appears in the dialed NPA and dialed number fields.

The SSP must be able to associate the new call codes received from the SCP database with the new structure codes which are being added for this capability. Additional billing flexibility is provided by allowing new database features to be added without requiring program changes in the SSP. A recent change view is used to associate the AMA call types received in the response message from the SCP data base with the proper AMA structure code.

11.8.4.4 Special Considerations for 800 Number Service

Since toll-free Service Access Code (SAC) calls (such as 800 or 888 calls) are free to the originating party, any coins deposited for toll-free SAC calls originating at a coin station should be returned to the calling party. The coins are not returned until the end of the call.

While coin charging can be reviewed as a type of billing, it is actually implemented in the SSP feature control.

Message registers do not register calls from hotel and motel stations. Message rate customers are not pegged for message unit toll-free SAC calls. Also, no billing is performed for "Charge-A-Call" service for toll-free SAC calls.

As final carrier selection for toll-free SAC calls is ultimately determined by the SCP database, customers are prohibited from dialing 10XXX before a toll-free SAC number.

Line access to the SSP/800 capability can be selectively blocked through screening. Before launching a query to the SCP database, line and translation data are used to access screening forms. If a specific route index is specified, the call is terminated to that destination without accessing the SCP database.

11.8.4.5 SCP Database Communication

11.8.4.5.1 SSP Switch Query Message

When an incoming call is identified as a toll-free Service Access Code (SAC) number service call (such as an 800 or 888 number call), the appropriate data is passed to the TCAP message processor to be formatted into an initial query message. The data required to format a query message includes the following:

- (a) The originating transaction identification (ID) (assigned by the switch)
- (b) The dialed digits

- (c) The ANI digits
- (d) The LATA number
- (e) The originating station type.

11.8.4.5.2 Normal Response to SSP Messages

The information returned in the response message from the SCP database determines the action to be taken on a given call. The information in the response message includes the following:

- (a) The responding transaction ID (identical to originating transaction ID)
- (b) The carrier identification (local exchange carrier or IEC)
- (c) The network routing number (directory number)
- (d) Billing information (AMA call type and service feature ID).

A second component that may be included in the response message from the SCP is an ACG component. The information in the ACG component includes the following:

- (a) A 6- or 10-digit number
- (b) The control cause identification (reason for the ACG)
- (c) The duration (number of seconds control is to be active)
- (d) The normal gap interval (gap interval to be used for the control).

A third component that may be included in the response message from the SCP database is **send notification** component. This component contains echo data in the form of 4 bytes of information that is saved by the switch and returned to the SCP database when the call is completed.

11.8.4.5.3 Termination Notification Message

Upon receipt of a send notification component received from the SCP, the switch prepares a termination notification message to the SCP when the call terminates. Information needed for the termination message includes the termination indicator and the echo data.

Other optional data that may be included in the termination notification message is the connect time, an error code, or a problem data element.

11.8.4.5.4 Announcement Response to SSP Messages

If the SCP is unable to respond with routing instructions because of one of the irregular user actions, a **Play Announcement** message is sent to the switch. The play announcement message indicates the standard announcement to which the call is to be routed. It may also include an ACG component; however, no ACG controls are removed if the play announcement message does not contain an ACG component.

NOTE: The ACG controls are normally removed when there are no ACG components present.

Irregular User Actions: The switch provides the following announcements in response to irregular user actions:

- **Out-of-Band Announcement (1):** When a customer dials a toll-free Service Access Code (SAC) number, such as an 800 or 888 number, outside the calling band.
- **Vacant Code Announcement (2):** When a customer dials an unassigned toll-free SAC number.
- **Disconnected Number Announcement (3):** When a customer calls a recently disconnected toll-free SAC number.
- **Reorder (4):** When the SCP cannot determine whether the toll-free SAC number is unassigned or out of band.

In order for the caller to receive the proper tone or announcement, the switch must have the 10.17 View populated. The number in parenthesis is the ANNC CODE value and must be matched to an office RTI that provides the specified tone or announcement. Note that the requirements for SSP 800 also specify a tone of 5 and 6 for Busy Tone or No Circuit Announcement treatment. At present, there are no known applications returning this code; however, they could be populated in anticipation of when they are returned.

A fixed route should exist on View 10.1 for each of the announcements. View 10.17 can then point to the same RTI populated in View 10.1.

11.8.4.5.5 Error Conditions

Error condition responses are as follows:

- **Invalid Data:** If the SCP is unable to provide routing instructions because of improper or invalid data in the query message sent from the SSP, one of the following error messages will be returned:
 - Unexpected sequence of operations
 - Unexpected data element value
 - Data unavailable.
- **Protocol Error:** If a protocol error occurs in the query message sent to SCP by SSP, the SCP sends a reject message. The reject message includes a problem code to indicate what the problem is. A reject message is sent from SSP to the SCP if a protocol error is found in a response message. However, if a send notification component has been received and understood, a problem code which indicates the type of protocol error is included in the termination notification message sent to the SCP when the call is terminated.

A reorder tone or announcement is provided to the caller if one of the error messages is received by the switch, if the message is unable to complete the call as requested by the response message, or if the contents of the response message are not valid.

11.8.4.5.6 Routing

Routing instructions returned to the switch from the SCP database may be of three types:

- Translated intra-LATA routing
- Translated inter-LATA routing
- Untranslated toll-free Service Access Code (SAC) number (such as 800 or 888 numbers) routing.

In all cases, consistency checks between SCP-provided and switch data are performed. Failing checks will result in

the call receiving final treatment.

In the translated cases, office options determine:

- (a) Whether the returned NPA is deleted from the DN before being run through digit analysis, and
- (b) Whether to use the originating DAS or a toll-free SAC-dedicated DAS for digit analysis.

11.8.4.5.6.1 Intra-LATA Routing

Intra-LATA routing is determined first by obtaining routing information from the successful translation of the SCP-returned DN. To allow greater flexibility and more routing control, this routing information may be overridden by routing information on the carrier form for the pseudo-carrier indicated by the SCP database.

11.8.4.5.6.2 Inter-LATA Routing

Inter-LATA routing is determined solely on the routing information obtained from the carrier form associated with the SCP-provided carrier. Digit analysis is involved only to derive other, non-routing information necessary for call completion.

11.8.4.5.6.3 Toll-Free Service Access Code (SAC) Call Routing

When the SCP returns the toll-free Service Access Code (SAC) number (such as an 800 or 888 number) back to the switch, it is interpreted to mean that the SCP does not wish to translate the toll-free SAC number in question. A carrier must be returned to the switch in this case and its associated routing information is used to route the call. Digit analysis is not invoked.

NOTE: Toll-free service is not limited to the 800 NPA if the switch has implemented a toll-free treatment feature which allows additional toll-free Service Access Codes (SAC) such as 888 or 877.

11.8.4.6 Interface with Recent Change and Verify Subsystem

The SSP capability requires additions and modifications to recent change. The telephone company is able to add, delete, or modify the following via recent change and verify:

- Assign an NPA and an NXX to each trunk group from a non-EAEO handling toll-free Service Access Code (SAC) calls (such as 800 or 888 calls).
- Assign an NXX to each trunk group from an EAEO handling toll-free SAC calls.
- Assign an NPA to each trunk group from a tandem office handling toll-free SAC calls.
- Assign a LATA number to each trunk group from an end office or a tandem office handling toll-free SAC calls if the access tandem serves more than one LATA.
- Assign a LATA number for each end office SSP.
- Mark incoming trunk groups handling toll-free SAC calls as CAMA and non-CAMA.
- Designate for each IEC whether traditional or equal access signaling is used.
- Designate which trunk group to an IEC is for toll-free SAC services calling.
- Designate the 0ZZ code to be sent to the access tandem for calls routed from an end office SSP via an access tandem office.

- Assign 3-digit codes to be interpreted as toll-free SAC calls from a coin station.
- Assign toll-free SAC-NXX numbers for those not treated as number service calls by the SSP.
- Match the AMA call types received with the appropriate AMA structure code.
- Designate non-CAMA trunk groups for toll-free SAC Service coin station calls.
- Assign NPA codes to be used with 00Y codes received from end offices.
- Assign 00Y codes to be associated with originating NPA codes.
- Assign NPA codes, NPA-NXX codes, and NXX codes to be treated as toll-free SAC Service calls.
- Assign the XXX code in the signaling sequence, KP-0ZZ-XXX-ST, to be used by the access tandem SSP to recognize toll-free SAC Service calls, and in the response message to identify calls to be completed by a local telephone company.
- Match the announcement code in the response message with the proper announcement (See "Announcement Response to SSP Messages," Section 11.8.4.5.4).
- Assign a value for "R" in the 01R field in the international signaling.
- Assign 1NX codes for each international and consolidated carrier for IN calls using international signaling.
- Assignment of NS RTI and NS CDI for pseudo-carrier (routing overriding)
- Assignment of INH SCP NPA DEL (NPA inhibition from deletion by global parameter) Assignment of Digital Analysis Selector (DAS) for translating SSP/800 returned DN (See "Toll-Free Service Access Code (SAC) Call Routing," Section 11.8.4.5.6.3).

11.8.4.7 Measurements

11.8.4.7.1 New Traffic and Plant Measurements

With no usage counts required, all new counts are office totals. The existing 30-minute traffic reports include toll-free Service Access Code (SAC) service calls (such as 800 or 888 calls). New SSP feature counts are as follows:

- Toll-free SAC service (and other number service) calls originating at the switch
- Number service calls received from other offices at the access tandem
- Total toll-free SAC service calls
- Total toll-free SAC queries sent
- Failure to receive second signaling stage on equal access trunks
- Call processing failures before initial query
- Call processing failures after initial query
- Network management control block calls
- Signaling failure - time-out at the SSP

- Invalid command messages
- Abandon - before outpulsing
- Abandon - after outpulsing.

The following existing counts also contain information on number service calls:

- Failure to obtain ANI on a CAMA trunk at access tandem SSP
- All trunks busy or blocked in a group to an IEC.

See 235-071-100, *Traffic & Plant Measurements, Appendix 1*, for more details.

11.8.4.7.2 Miscellaneous Measurement Requirements

The 5-minute surveillance network management counts sent to EADAS/NM and ON-SITE systems are as follows:

- Total originating toll-free Service Access Code (SAC) service (such as 800 or 888 numbers) attempts
- SCP-blocked toll-free SAC Service calls due to vacant codes
- SCP-blocked toll-free SAC Service calls due to overload
- SCP-blocked toll-free SAC Service calls due to mass calling
- SCP-blocked toll-free SAC Service calls due to manual control
- Control list overflow counts - includes the following counts:
 - 6-digit vacant code list
 - 10-digit vacant code list
 - Nonpurchased NPA code list
 - SCP overload code list
 - Mass calling code list
 - Manual control code list.

11.8.4.8 Service Switching Point Testability

11.8.4.8.1 Service Switching Point Information

The SSP testing information provided here includes the following:

- **Test Query Procedures:** This allows switch personnel to use the SS7 and TCAP to launch queries for the following:
 - SSP to SCP interface testing

Verifying the data associated with a query.

- **Event Trapping Facility:** This enables switch personnel to trace the call processing events within the switch.
- **Extra Measurement Counts:** These are a part of the event trapping facility. These assist switch personnel in resolving network problems.

11.8.4.8.2 Service Switching Point Test Query

The SSP test query is a manual test run when a new switch is installed with SSP capability or an existing switch is retrofit with SSP.

The following are the SSP test query requirements:

- The office personnel manually generates the SSP test at the switch via an input message.
- The results of the test are displayed at the input/output (I/O) channel where the test was initiated.
- The switch only allows one test message to be active at a time. This includes both SSP test queries and direct signaling test queries.
- A test message is sent even if an ACG control is active on the SSP number in the query.
- The test result includes the global title from the original input message.

11.8.4.8.3 SSP Test Query Sequence

The test query flow is as follows:

- Switch personnel launch a test query via an SSP test call input command:
`TST:NS800=a, ANI=b, LATA=c;`
- The query is processed; the SSP launches the query to an SCP database and waits for the response.
- The SCP processes the query just like a regular SSP query. A reply is formatted and returned to the SSP.
- The returned reply is processed and the contents displayed on the read-only printer (ROP) for switch personnel.

11.8.4.8.4 Event Trapping

The event trapping for the SSP capability provides a mechanism for informing office personnel of specified events occurring in the switch. The purposes for providing event trapping are as follows:

- To obtain additional information concerning a problem event, to assist in classifying and correcting the problem
- To allow the office personnel to determine which of several events occur that effect a common count.

Table 11.8-4 indicates specific events that are trapped, in which processor the event is trapped, and the indication of additional data displayed when the event occurs. Specific requirements of the existing system include the following:

- Switch personnel activate a trap for an SSP event via an input message.

- When the trap is triggered by the event, the output is displayed on the ROP.
- Only one trap is activated with each input message.
- Individual traps or all traps can be turned off with a single input message.
- Traps have a maximum duration of 30 minutes and a default of 10 minutes.

Existing trapping mechanism is used as a foundation for the new traps. The only new requirement to the trapping mechanism needed for SSP is the ability to display additional data when the trap is reported to switch personnel.

11.8.4.8.5 Test Query Limits, Restrictions, and Capabilities

The test query facility expects the same 3-second query response turnaround as the base SSP capability. Only one active test query is allowed at a given time. The test query is handled and launched into the CCS network, regardless of any network management ACG controls in existence.

Event trapping output is prevented from overloading the Master Control Center (MCC) and ROP by throttling mechanisms.

11.8.4.8.6 Interactions

Queries use the CNI ring for access to the CCS direct signaling network. Event traps do not interact with any other capability other than SSP. Existing tables, message handlers, and throttling mechanisms will be expanded to include SSP requirements.

Table 11.8-4 Trapping SSP Events

EVENT	PROCESSOR		ITEM DISPLAYED
	NO DLN	DLN	
NM Blocked	AM	DLN AM	Called Number SM
Returned Query	AM	DLN	Called Number Failure Source
Reject Message	SM		Called Number Problem Code
Return Error	SM		Called Number Error Code
Time-Out	SM		Called Number
Play Announcement	SM		Called Number Announcement Code
Send Notification	SM		Called Number DPC + SSN
Termination Notification	SM		Called Number DPC + SSN
ACG Component Received	AM	DLN	Controlled Number Duration Value Gap Value

11.8.5 Feature Interactions

11.8.5.1 Account Codes

A user with an account code feature can invoke account code procedures before dialing an SSP/800 number. However, SSP/800 AMA records have no provisioning in their structure for storing the account code, so the feature loses its effectiveness. AMA restrictions for ACCT are ignored for SSP/800 calls, as no AMA records are made for the originator.

For additional interactions, see "Message Detail Recording (MDR)," Section 11.8.5.3 .

11.8.5.2 Authorization Codes

A user with an authorization code feature can invoke authorization code procedures before dialing an SSP/800 number. However, no AMA records are made for the originator of SSP/800 calls.

A user can provision ATH FIRST=Y on their line and dial an SSP/800 number. If ATH procedures were not invoked first before dialing the SSP/800, a query will launch and the call will fail when the response comes back from the SCP.

For additional interactions, see "Message Detail Recording (MDR)," Section 11.8.5.3, and "Individualized Dialing Plan (IDP)," Section 11.8.5.4.

11.8.5.3 Message Detail Recording (MDR)

A line assigned with an MDR feature and a group capable of recording public MDR records will create a PUBLIC MDR record when an SSP/800 call is made. Any ACCT or ATH code entered in the course of the SSP/800 call can be recorded in the MDR record. ACCT for MDR and ATH for MDR are currently supported. A user can be prompted for an ACCT or ATH code if the SSP/800 call will generate a public MDR record and the user has the MDR RSTRCT (ACCT) or ATH for MDR restriction set.

11.8.5.4 Individualized Dialing Plan (IDP)

An escape to POTS code can be dialed before an SSP/800 number and can be marked as DPAT restricted. If the user has an ATH code feature, the user will be prompted for an ATH code after the SSP/800 query is launched and the SSP/800 response comes back. The ATH code can override the DPAT restriction. Intercom dialing can be set up such that a user can dial an abbreviated digit string which can be rebuilt into an SSP/800 number.

11.8.5.5 Display: Per-Call Privacy

Per-call privacy can be invoked before the SSP/800 number is dialed. This privacy can be maintained to the terminating port.

11.8.6 ASP Enhancements to Support Toll-free Services

Within the North American telecommunications market, toll-free calls, that is 800 or 888 calls, are today handled by an Intelligent Network Architecture. This IN/1 architecture makes use of the service specific Service Control Point (SCP) databases and Service Switching Point (SSP) software in switching systems. The SSP capabilities are known interchangeably as SSP/800, Number Services (NS), and NS-800.

The supply of toll-free numbers within the 800 Service Access Code (SAC) is exhausted. This new AIN Toll-free feature provides an Advanced Intelligent Network (AIN) based Toll-free Service using the Advanced Services Platform (ASP) capability. The AIN toll-free feature allows any number to be marked as a toll-free number, thereby eliminating the restriction of using 800, 888, or 877. Advanced Services Platform provides toll-free service in a manner which operates as transparently as possible to the existing SSP/800 capabilities.

Transparency is essential so that the calling party and carrier perceive no difference in the SSP/800 service.

The ASP query to the SCP contains the same call information parameters as a SSP/800 query. The ASP Toll-free query can be handled by the SCP using either of the following available methods:

- (1) An AIN SCP equipped with service logic to support AIN Toll-free calls.
- (2) A protocol conversion mechanism acting as a front end to the existing SSP/800 database.

The response from the SCP must be an ASP R0.1 response that contains the toll-free parameter information necessary to deliver the call. The ASP Toll-free Service is being developed in compliance with GR-2892-CORE.

The AIN Toll-free feature is not intended to provide transparency from a service provider perspective since this feature is provided on an AIN platform instead of the existing SSP/800 platform.

The AIN Toll-free feature is deployed in two phases:

Phase 1 (feature 99-5E-3151) provides the AIN-based Toll-free functionality.

Phase 2 (feature 99-5E-3260) provides enhancements to measurements and an increase in size of the Automatic Call Gapping (ACG) list.

These are secured features and a right-to-use (RTU) fee must be paid to Lucent Technologies before enabling information is provided.

See 235-190-126, *Advanced Service Platform Release 0.1B* for details about both features.

11.9 SSP800/ASP 0.1B INTERWORKING FEATURE

11.9.1 Description

The Service Switching Point 800 (SSP800)/Advanced Services Platform (ASP) Release 0.1B Interworking feature is an enhancement to the SSP800 Number Service feature and allows the transition from Advanced Services Platform (ASP) to SSP800 within the processing of a call. It does not have a Right to Use (RTU) fee.

NOTE: 800 Service is not limited to the 800 NPA if the switch has implemented a toll-free treatment feature which allows additional toll-free Service Access Codes (SAC) such as 888 or 877.

In response to an ASP Rel 0 or 0.1 protocol query, the Service Control Point (SCP) may return a routing message, specifying use of the LEC/Pseudo Carrier, and a routing number that translates to a Number Services Code (in other words, an SSP800 number). Billing is generated at the end of the call, not at the transition. In this case, the SSP800 feature will be invoked, and an SSP800 query will be sent to the appropriate SCP.

11.9.2 Background

Prior to release of this special feature, an attempt to return such a response to an ASP query would have resulted in error treatment on the call.

Before the SSP800/ASP 0.1B Interworking feature was available, the following transitions were allowed between triggers:

- SSP800 to ASP and
- ASP to ASP.

With the release of this feature, the following transitions are now allowed between triggers:

- SSP800 to ASP,
- ASP to ASP, and
- ASP to SSP800.

Note that although SSP800 to SSP800 is not allowed, this feature does allow multiple SSP800 triggers on a single call, if an ASP trigger intervenes. In other words, SSP800 to ASP to SSP800 transitions may occur.

11.9.3 Availability

The SSP800/ASP Release 0.1B Interworking feature is a software update to the 5E9(1) software release, and is included in 5E9(2).

11.9.4 Feature Environment

The SSP800/ASP Release 0.1B Interworking feature is provided on a per-switch basis.

11.9.5 Feature Operation

Except for cases specifically stated in the following text, the individual ASP and SSP800 features continue to operate independently, with no impact on each other.

Before this feature, when SSP800 was detected after an ASP (Feature Code Dialing (FCD) or ASP Customized

Dialing Plan (CDP) trigger, ASP would be ignored, and an SSP800 query would be launched. With this feature installed, dialing SSP800 digits after an FCD or CDP trigger will result in an ASP query with the SSP800 digits stored in the Collected Address parameter for Release 0.1 protocol queries or Dialed Digits parameter for Release 0 protocol queries. The SCP must now be able to handle the SSP800 digits in the ASP query.

11.9.6 User Operation

This feature is transparent to the end user, and no special action is required by switch office personnel to activate it.

11.9.7 Engineering

11.9.7.1 Hardware Resources

No hardware considerations are associated with this feature.

11.9.7.2 Software Resources

No software considerations are associated with this feature.

11.9.7.3 Transition Considerations

This feature only applies to a 5ESS[®]-2000 switch that interfaces with an SCP that supports this feature. The SCP must be running ASP Release 0.1B.

11.9.8 Interactions

There are no new interactions associated with this feature.

11.9.9 Incompatibilities

There are no interactions associated with this feature.

11.9.10 Dependencies

This feature is an enhancement to the SSP800 Number Service feature.

11.9.11 Limitations

There are no additional limitations associated with this feature.

11.9.12 Isolation Constraints

Not applicable.

11.9.13 Feature Implementation

11.9.13.1 Office Data Administration Provisioning

There is no ODA provisioning associated with this feature.

11.9.13.2 Recent Change Provisioning

There is no RC provisioning associated with this feature.

11.9.13.3 Customer Premise Equipment

Not applicable.

11.9.14 Maintenance Considerations

Not applicable.

11.9.15 Administration

11.9.15.1 Measurements

The only measurement impacted by this special feature is the ASP "Serial Triggering Limit Exceeded" count which will be incremented if the SSP800 trigger causes the ASP Serial Triggering threshold to be exceeded. No other ASP or SSP800 specific measurements are impacted.

11.9.15.2 Billing

It is recommended that this feature be applied during lower traffic hours since the Call Record Remote Insert System Process (PID 32) will be purged when installing this SU. It is unlikely but possible that some billing records may be lost or that some records may contain invalid information due to the purge of the process.

When a transition from ASP to SSP800 occurs, the AMA records for any previous ASP call legs will be generated based on the billing instructions provided by the SCP in the corresponding routing response. Similarly, the AMA records for the SSP800 call leg will be created in accordance with the existing billing requirements. Billing for the individual call legs for ASP and SSP800 will not be impacted by the involvement of the other feature in terms of format and structure. Individual data elements of the SSP800 AMA Records will be impacted as listed in Table 11.9-1. For more information on billing, refer to 235-190-300, *Billing Features and Specifications*.

Table 11.9-1 SSP800 AMA Records Impacted By The SSP800/ASP Feature

SSP800 Billing	Populated From
Originating Number	(1) If previous ASP query was for an ASP subscribed originating trigger: • Originating Station DN from previous ASP R0 query, or • Calling Party ID from previous ASP R0.1 routing response, or • Calling Party ID from previous ASP R0.1 query (2) If previous ASP query was for an ASP non-subscribed originating trigger (e.g., a 3/6/10/N11 Trigger)—the digits on which the 3/6/10/N11 trigger was defined. (3) If previous ASP query was for an ASP subscribed terminating trigger (e.g., a TAT—the digits on which the TAT was defined.
Dialed Number	• Routing Number from previous ASP R0 response or • Called Party ID from previous ASP R0.1 response
Destination Number	Routing Number from SSP800 SCP response
Notes:	

- a. Originating Number could be a three-digit or seven-digit number as well as a ten-digit number if the previous ASP query was for a 3/6/10/N11 trigger.

11.10 LOCAL AREA SIGNALING SERVICE FEATURES

11.10.1 Feature Definitions

This section covers the use of SS7 by the various LASS features; therefore, only a brief description of each feature is provided. For more detailed descriptions and the customer interface with LASS, refer to 235-190-130, *Local Area Signaling Services Feature Document*.

11.10.1.1 Automatic Callback

The Automatic Callback (AC) feature provides the calling station with the ability to place a call to the last incoming call directory number. The call may not be able to be completed immediately due to the called DN being busy; however, the AC feature causes a switch to monitor the busy/idle status of the called number (scanning), and when the called number and the calling station are both found to be idle, the calling terminal is given a ringback alerting. When the ringback is answered, the call is set up to the called number.

11.10.1.2 Automatic Recall

The Automatic Recall (AR) feature enables a calling station to automatically place a call to the last party called from the calling terminal. If the called party is busy, the Automatic Recall feature causes a switch to monitor the busy/idle status of the called directory number (scanning). When both the calling and called numbers are idle, the calling terminal is given a ringback alerting. When the ringback is answered, the distant party is alerted.

11.10.1.3 Customer-Originated Trace

The Customer-Originated Trace feature provides the end-user the ability to trace the last incoming call after it has been successfully completed or when terminated before conversation has begun. An end-user can invoke a call trace through the customer telephone equipment, but does not receive the results.

11.10.1.4 Individual Calling Line Identification

Customers with the Individual Calling Line Identification (ICLID) feature and an analog or integrated services digital network (ISDN) display unit can see the calling party's directory number displayed before answering the call. This provides direct call screening.

The Individual Calling Line Identification feature works on any intraswitch call (except for intermodule non-SS7 trunk calls) and on any interswitch calls that originate from a switch that sends the calling TN to the terminating switch in the IAM. The Individual Calling Line Identification feature consists of two main components, **calling number delivery** (delivery of the calling directory number to the terminating station set) and **directory number privacy** (preventing delivery of the calling directory number to the terminating station set).

11.10.1.5 Screen List Editing

The Screen List Editing (SLE) capability is available to those customers having access to the LASS Selective Features [Selective Call Acceptance (SCA), Computer Access Restriction (CAR) Selective Call Rejection (SCR), Selective Call Forwarding (SCF), and Selective Distinctive Alert (SDA)], and is provided only if a client feature is assigned or is generally available.

The SLE capability allows LASS Selective Feature (LSF) users to create and modify lists of telephone numbers (TN) associated with the LSF assigned to their directory number (DN). If the calling party's DN is on the list, the call is given special treatment by the LASS selective features.

Screen List Editing interactively guides users in editing screening lists. A set of interactive recorded announcements are used for analog stations and ISDN stations. Additionally, display messages are provided for ISDN stations with

display capability. These announcements and ISDN displays can be customized.

11.10.1.6 Selective Call Acceptance

Selective Call Acceptance screens incoming calls and only allows calls to terminate if the calling party number matches a number on the Selective Call Acceptance screening list. If the calling party number is not on the screening list, the call routes to an announcement or forwards to a destination chosen by the user.

11.10.1.7 Computer Access Restriction

The Computer Access Restriction feature is similar to the Selective Call Acceptance feature, but is designed for controlling computer access of voice channel data (modem-to- modem) calls.

Computer Access Restriction allows a business or residential customer to restrict the access of calling parties to the customer's computer. If the telephone number of the calling party is not on the screening list, the call routes to an announcement or forwards to an alternate directory number depending on the user's selection prior to feature activation. The Computer Access Restriction customer does not receive any indication of the call.

11.10.1.8 Selective Call Forwarding

The SCF allows a residential or business customer to preselect which calls are forwarded based on the identity attribute of the calling party. The forward-to number is selected by the user during the screen list editing session.

11.10.1.9 Selective Call Rejection

The SCR allows a residential or business customer to reject calls from identity attributes which are on the customer's SCR rejection list. The identity attributes can be entered as the last call to alert the SCR customer. Alerting is defined as either ringing or applying call waiting tone to a terminating station. Calls that are rejected are routed to an announcement.

11.10.1.10 Selective Distinctive Alert

The SDA feature allows a residential or business customer to preselect which calls are to be provided distinctive alerting treatment based on the identity attributes of the calling parties. The identity attributes can be entered directly (dialed in) by the SDA customer, or entered as the last call to alert the SDA customer. Alerting is defined as either ringing or applying call waiting tone to a terminating station.

11.10.2 ISDN User Part Signaling

The proper operation of the LASS features (described in "Unsuccessful Call Setup Procedures," Section 5.3.3) requires that interswitch calls be set up by the SS7 call setup and clearing procedure. The LASS feature requires that the calling DN, uniqueness, and privacy indicators be transported between switches.

11.10.3 Signaling Connection Control Part (SCCP)

This part provides specialized routing capabilities and defines the class of signaling connection service for transporting the CCS direct signaling messages to and from the SS7 network.

- The TCAP queries and unidirectional messages determine the destination point code and subsystem number via global title translation at an STP.
- The TCAP response to queries and conversation messages routed via signaling point code and the subsystem number in the calling party address parameter of the received TCAP messages. Delayed responses for terminating scanning are an exception to this rule; they are routed by global title. There are two response messages in this category: called party idle and timer expired.

11.10.3.1 SCCP Unit Data Message

11.10.3.1.1 Transaction Capabilities Application Part Protocol

This protocol is used for transmitting noncircuit-related messages over the SS7 network between two signaling nodes to assist the Local Area Signaling Service. The TCAP is contained within the data field of the SCCP unit data message. The TCAP provides the application data required for processing the call.

The TCAP message can be viewed as a collection of elements. The elements consist of an identifier, length, and contents. One group of these elements make up the transaction portion of the message and another group makes up the component portion.

11.10.3.1.1.1 Transaction Portion

The transaction portion provides the receiving node with:

- (1) Information specifying whether the transaction requires multiple messages via the package type which identifies them as one of the following interactions:
 - Query with permission
 - Query without permission
 - Conversation with permission
 - Conversation without permission
 - Response
 - Unidirectional.
- (2) A Transaction ID to associate incoming messages to a specific transaction. There are two types of transaction IDs. The originating transaction ID field is four bytes in length and is assigned by the originator of the transaction. The value is returned as responding transaction ID if the transaction provokes a response from the receiving node. The responding transaction ID is also four bytes in length and is the originating transaction ID from the message provoking the response.

11.10.3.1.1.2 Component Portion

All TCAP messages contain one or more components. Components specify the operation that is to take place, or the results of an operation.

The component types possible are:

- Invoke: Used to cause operations to be performed. Included in this component is an operation code to indicate an operation family and a specifier to identify a specific operation within the family.
- Return result: Returns a result of an invoked operation. Contained in this component is a parameter set to return the necessary data. This is only used if operation was successfully completed.
- Return error: Reports the unsuccessful completion of an invoke operation. Included in this component is an error code that provides the reason for a failure.

- **Reject:** Reports the receipt of a component with a protocol error. Included here is a problem code used to detail the problem in the incorrect component received.

The return error and reject components contain an error code and a problem code, respectively. The return error component reports the unsuccessful attempt of an invoked operation. The error code provides the reason for the failure. The reject component, used to report receipt of incorrect message or component, has a problem code to detail the problem.

Operation code specifiers required can be one of the following:

- For operation family: miscellaneous
 - Queue Calling Directory Number
 - Dequeue Calling Directory Number
- For operation family: send notification
 - When party is free
- For operation family: operation control
 - Cancel.

Each TCAP component must have a parameter set. Parameters are used to transport information to perform operations or to report the result of operations. The content section of the parameter set may be empty, depending on the operation requested.

- Busy/idle status
- Call forwarding active
- DN to line service type mapping
- Terminating restrictions
- Duration
- Digits - calling DN.

11.10.3.1.1.3 Errors

Errors are used to report data and application-specific errors. Error codes can be as follows:

- Unavailable resource
- Task refused
- Queue full
- No queue

- Not queried
- Timer expired.

11.10.3.1.2 CCS Network - Routing Errors

If the originating switch sends out an initial SS7 TCAP query to an STP and the TCAP message cannot be routed to the appropriate SCCP user, a unit data service (UDTS) message is returned to the originator that contains the following information:

- Called Party Address
- Calling Party Address
- One of the following diagnostics:
 - No translation for an address as shown
 - No translation for this specific address
 - Subsystem congestion
 - Subsystem failure
 - Network congestion
 - Network failure
 - Unequipped user
- Returned user data.

11.10.3.2 TCAP For Automatic Callback/Automatic Recall

11.10.3.2.1 Message Flow for Terminating and Originating Scanning

The SS7 message flow is the same for the Automatic Callback and Automatic Recall features. An initial query is sent and a response is returned to determine if the feature activation is allowed. If the originating switch determines that the feature activation is allowed, it next determines if the originating or terminating scanning is to be used. It then continues until deactivated by time-out, cancellation, or ringback.

Figure 11.10-1 shows the message flow through the SS7 network for terminating scanning. Figure 11.10-2 shows the message flow for originating scanning.

11.10.3.2.2 TCAP Messages - Terminating Scanning

If terminating scanning is required, the originating switch sends a TCAP query to request the terminating switch to perform terminating scanning. The terminating switch must be capable of performing this function as well as having the resources available to do it.

11.10.3.2.3 Terminating Scanning - Cancel Request

If the Automatic Callback and Automatic Recall feature timer expires at the originating switch, or if the feature

activation is canceled by the end-user, a cancel message is sent to the terminating switch to cancel the terminating scanning request.

11.10.3.2.4 Terminating Scanning - Timer Expired

If the feature timer at the terminating switch expires before the called DN is idle, the terminating switch sends a timer expiration message to the originating switch.

11.10.3.2.5 Dequeue Message Following Terminating Scanning

After a ringback has been answered, the originating terminal sends a **dequeue** message to remove the calling DN from the queue.

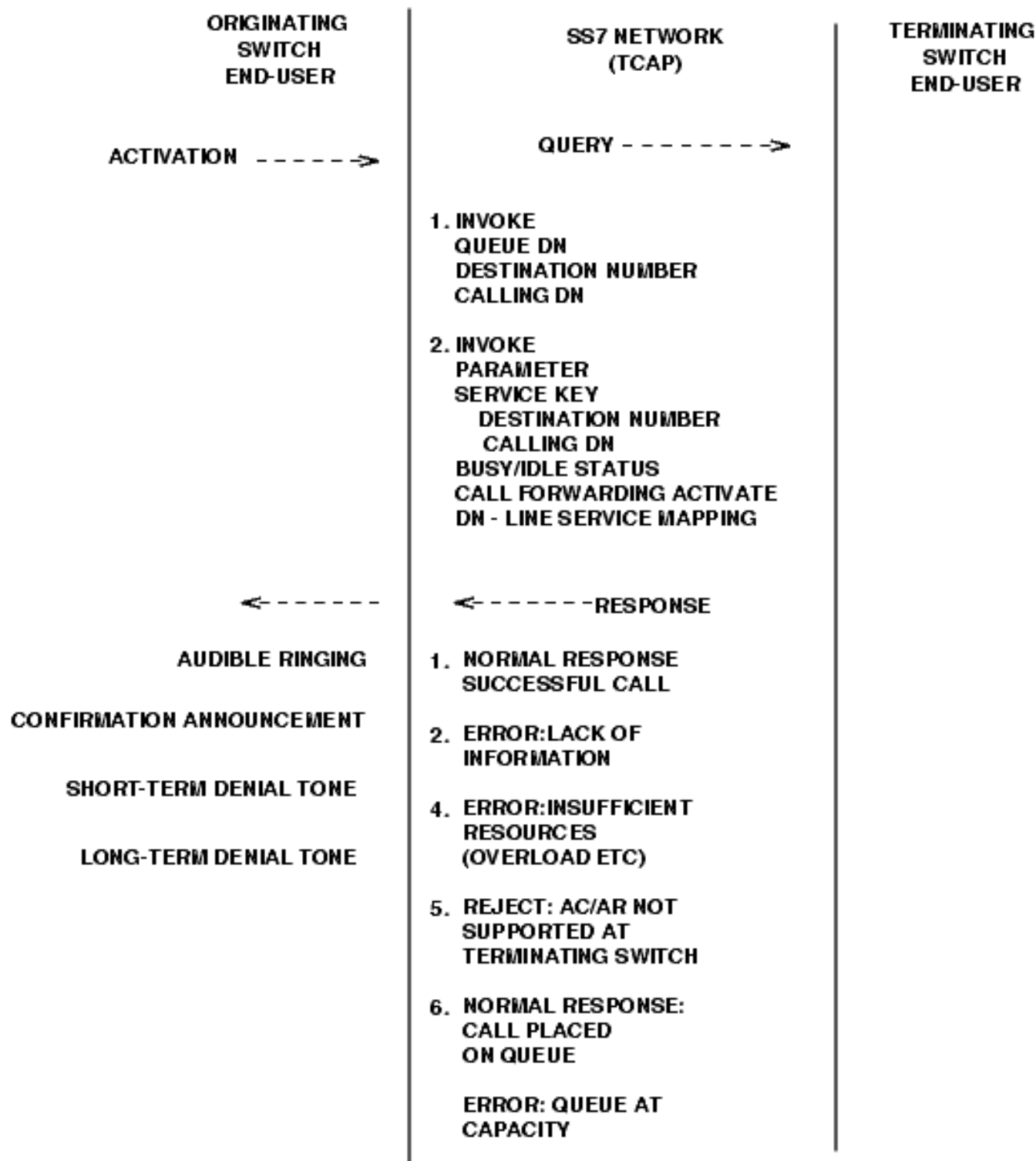
11.10.3.2.6 SS7 TCAP Messages - Originating Scanning

If originating scanning is done because the office parameter is set to perform originating scanning or if the terminating switch sends an error message when queried to perform terminating scanning, a series of busy/idle status queries are sent from the originating switch to the terminating switch. These busy/idle status queries are sent at intervals prescribed by the originating scan rate timer.

11.10.3.2.7 Dequeue Message Following Originating Scanning

Just as for terminating scanning, after a ringback has been answered, the originating terminal sends a **dequeue** message to remove the calling DN from the queue.

Responses to the busy/idle status queries from the terminating switch may be busy/idle status, data unavailable, or task refused.



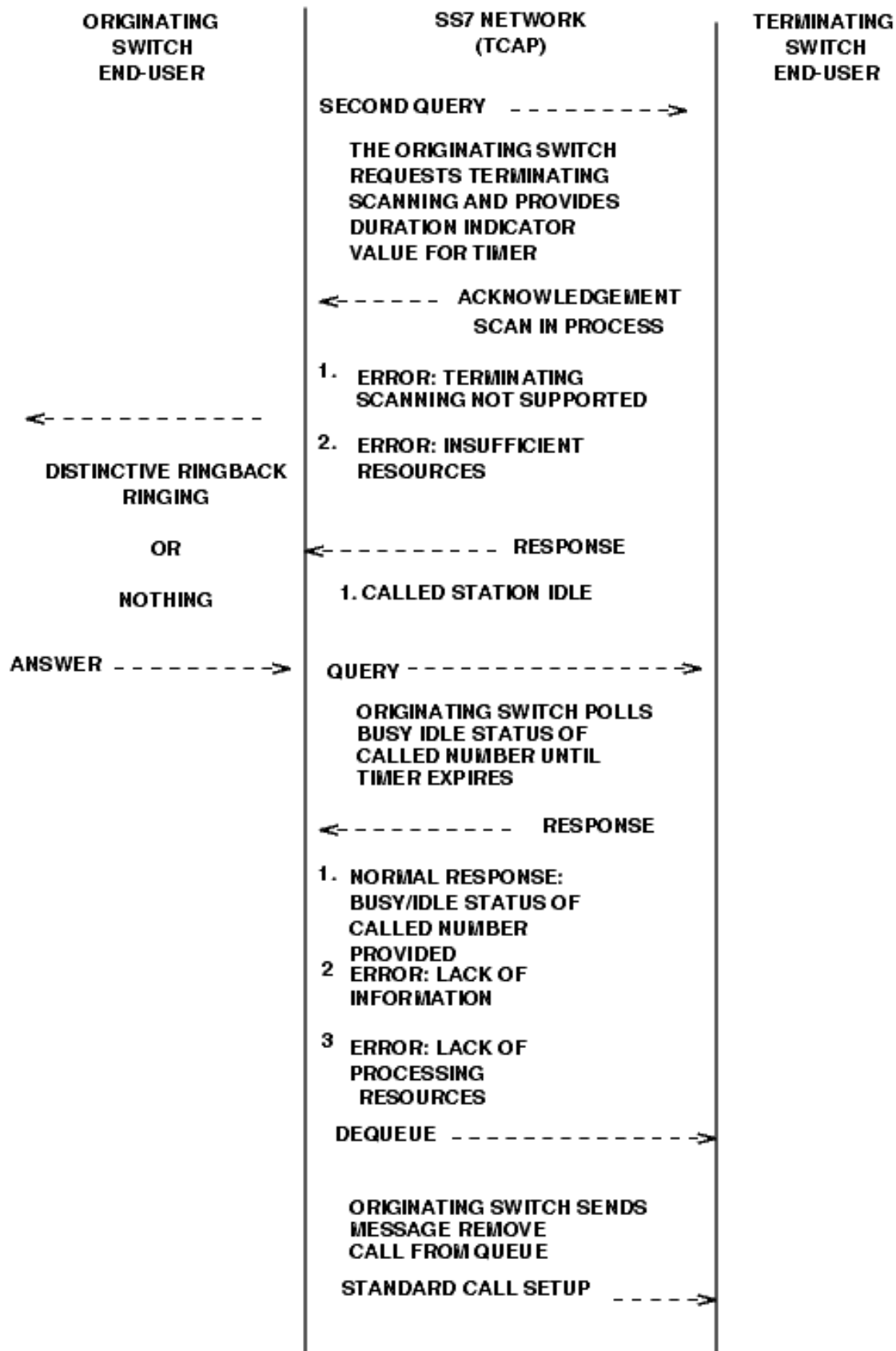
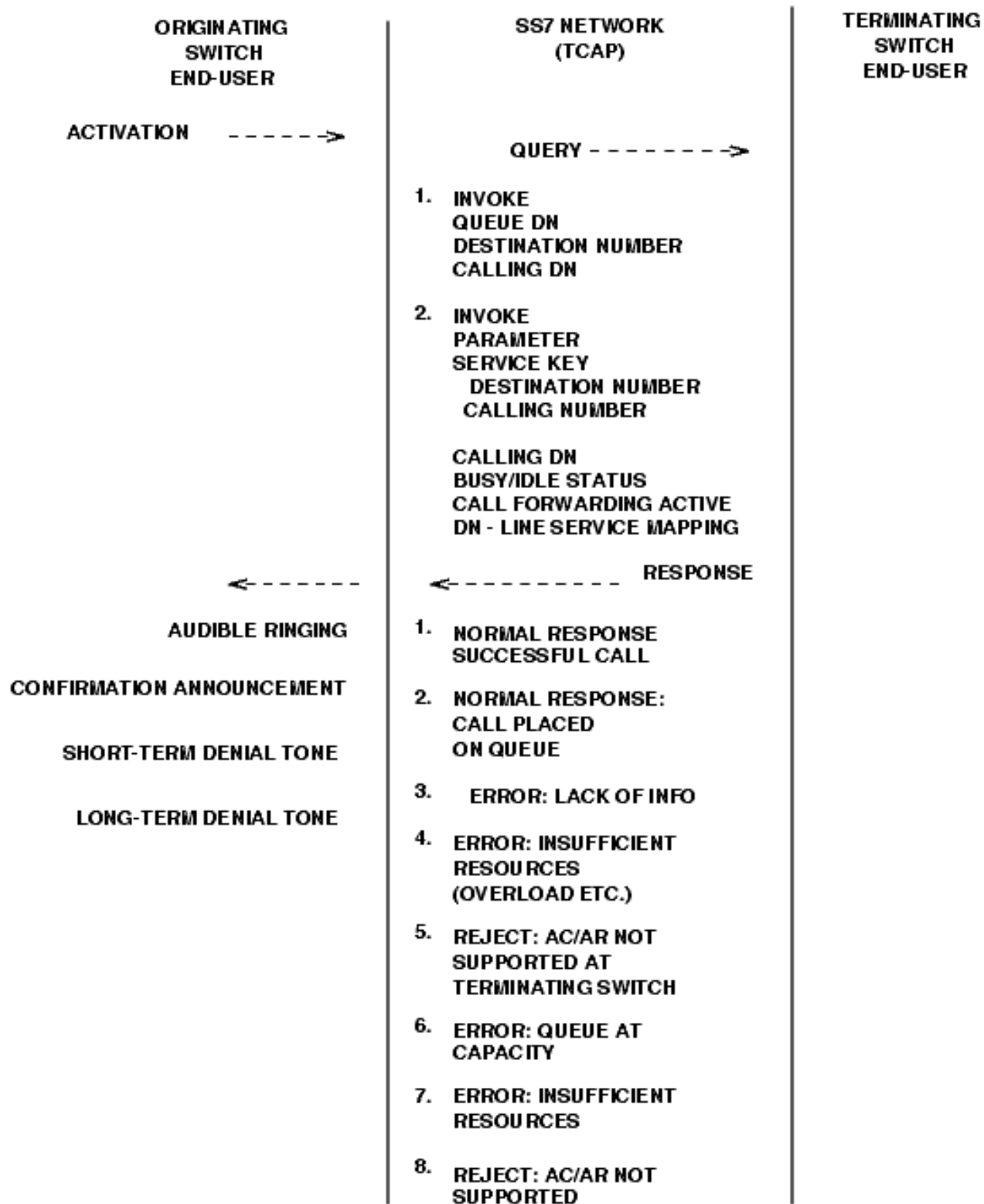


Figure 11.10-1 TCAP Message Flow for Terminating Scanning



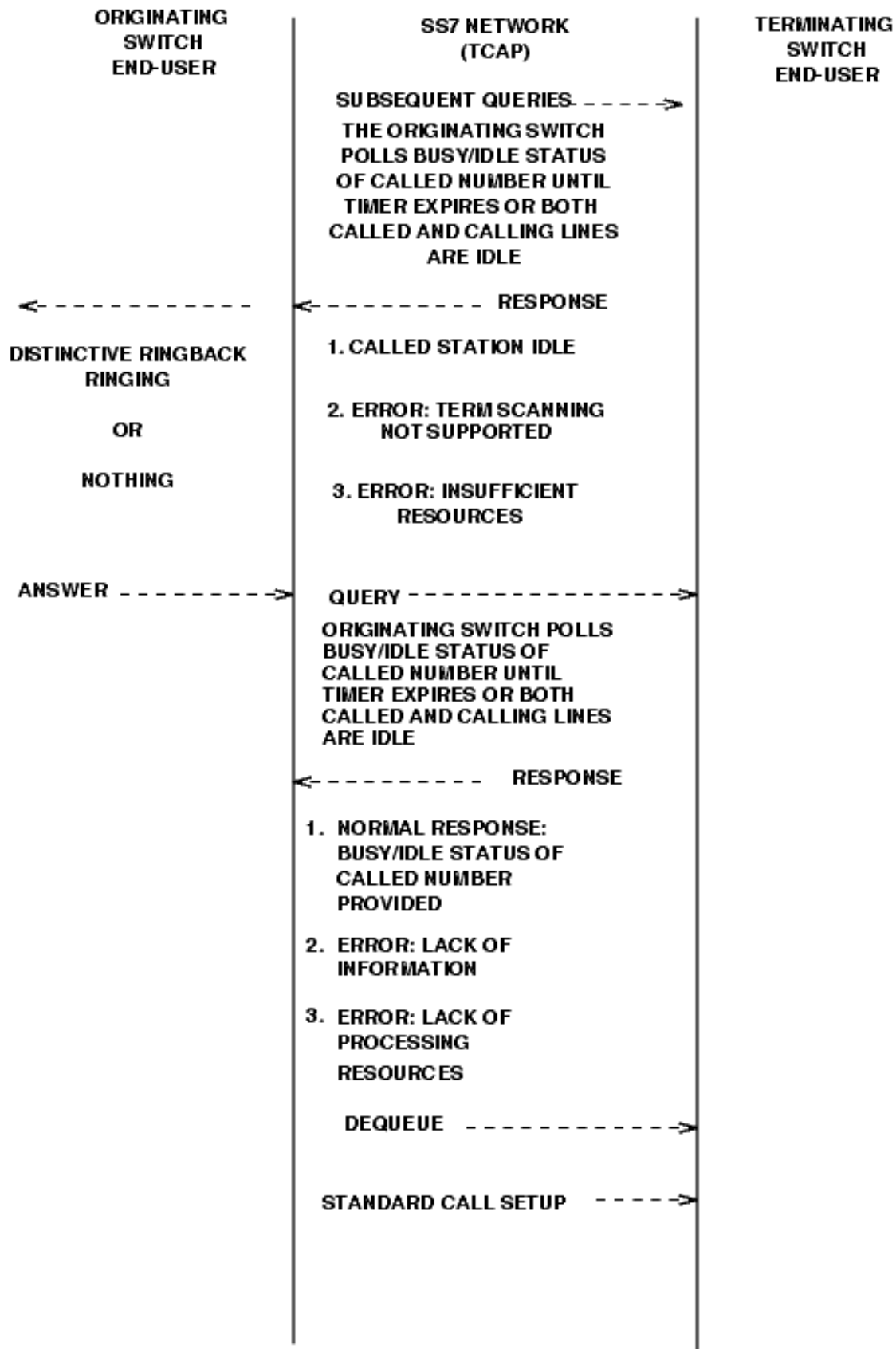


Figure 11.10-2 TCAP Message Flow for Originating Scanning**11.10.4 Screen List Editing Identity Attribute Validation****11.10.4.1 Identity Attribute Assigned at the Serving Switch**

Screen List Editing validates all entries made to screening lists. Validation ensures that callers can be successfully identified so that calls from them can be screened. The following is checked for every screen list entry entered:

- Is the screen list entry assigned to a line?
- For screen list entries not assigned at the user's switch, does the switch serving the entry have SS7 connectivity? (Without such connectivity, the switch cannot determine the validity of the calling party's number when a calling number is added to the list).
- Does the screen list entry match the number provided when the station being identified makes a call? (For example, a number assigned to a multiline hunt group line may not, in some cases, be sent as the calling party number.)
- Can the station being identified make calls to the user? (For example, the station may be fully restricted for originations and not be in the user's terminal group.)

The SLE feature makes use of SS7 TCAP protocol in validating screen list entries not assigned at the user's switch. If no checks fail, the number is added to the screening list and a confirmation announcement is given. Otherwise, the number is not added and an appropriate error announcement is provided (UNAVAIL, ADDLATER).

11.10.4.2 Identity Attribute not Assigned at the Serving Switch

The serving switch formats a TCAP query including the 10-digit destination number (the identity attribute) and the 10-digit calling directory number (the user's number). The query requests that two parameters be specified by the far-end switch for the identity attribute.

- (1) DN-to-Line-Service-Type Mapping - This parameter consists of directory number match and line type.
- (2) Originating Restrictions. If the serving switch is unable to send a query due to lack of resources, the user is given a short-term error announcement, if possible. If the resources to provide the short-term announcement are not available, the user is given a standard error treatment and the identity attribute is not added to the list.

11.10.4.2.1 Sending a TCAP Query

One of the purposes of the SS7 query is to verify that two switches have SS7 connectivity. Without such connectivity, the calling party directory number is not available for screening when a call is made to the user. If the SS7 STP indicates to the serving switch that the far-end switch lacks SS7 connectivity, the identity attribute is not allowed on the screening list. The STP may also indicate that the query cannot be delivered due to abnormal network conditions.

11.10.4.2.2 Receiving the TCAP Query

If the far-end switch receives less than the 10 digits for either number, it returns a response message with an error value of "unexpected value."

If the query message contains protocol errors in content or format, the far-end switch returns a reject message with an appropriate problem specifier.

11.10.4.2.3 Determining a Response

Once a query is received in correct form, the far-end switch retrieves information on the identity attribute. If the switch lacks the resources to process the query and respond to it, the switch attempts to return a response message with an error code of Task Refused. Neither the Originating Restriction nor the DN-to-Line Service-Type Mapping parameter is provided in this message.

If the identity attribute is assigned, it passes the directory number match check. Table 11.10-1 indicates whether a match or no-match is expected for a particular service type. Regardless of the expected value, the switch checks for the directory number match for all identity attributes to be added. The switch compares the identity attribute with the number provided in the calling party number parameter of the SS7 initial address message when the calling party places an interswitch call.

Table 11.10-1 Expected DN-Match and Line Type Values

SERVICE TYPE	DN-MATCH ^a	LINE TYPE
Coin DN	Match	Coin
Coinless Public DN (Such as Charge-A-Call)		Match
2-party DN with ANI	Match	Individual
2-Party DN without ANI	No Match	Multiparty
2-Wire Individual DN	Match	Individual
4-Wire Individual DN	Match	Individual
BRI Individual DN	Match	Individual
Analog Attendant DN (Without Multiple Position Hunt)	Either	Individual
Emergency Bureau DN	Either	Individual
Hotel/Motel DN	No Match	Nonspecific
Direct Connect DN	Match	Individual
Manual DN	Match	Individual
Multiparty DN (More than Two Parties)	No Match	Multiparty
Multiline Hunt Group (Regular, Circular, UCD) Group DN	Either	Multiline Hunt
Multiline Hunt Group (Regular, Circular, UCD) Member Hunt DN	Either	Multiline Hunt
Multiline Hunt Group DN (Regular, Circular, UCD) Member Non-Hunt DN	Either	Multiline Hunt
Multiple Position Hunt - Subgroup 1 DN	Match	Multiline Hunt
ISDN Attendant - Subgroup 1 DN	Either	Multiline Hunt
ISDN Attendant/Multiple Position Hunt Other subgroup DN	No Match	Multiline Hunt
ISDN Attendant Member Start Hunt DN	Either	Multiline Hunt
ISDN Attendant Member Non-Hunt DN	Either	Multiline Hunt
Operator DN	Either	Individual
PRI PBX DN	No Match	PBX
Extended Digital Subscriber Line Hotel/Motel DN	No Match	PBX
Non-PRI PBX DN (PBX with Line Appearance)	Either	Individual
Non-PRI PBX DN (PBX with Trunk Appearances)	No Match	Nonspecific
DN with ISDN Shared Call Appearances	Match	Individual
Series Completion DN	Match	Series Completion
Unassigned DN	No Match	Unassigned DN
All Others	No Match	Nonspecific
Notes:		
a. Where "Match" or "Either" is indicated, DN-Match must be checked explicitly.		

11.11 TCAP IMPROVEMENTS FOR A SWITCH SPANNING MULTIPLE LATAs

11.11.1 Feature Description

The transaction capabilities application part (TCAP) improvements for switch spanning multiple local access transport area (LATA) feature, number 99-5E-2708, permits lines (or groups of lines) to be assigned a LATA number different from the default LATA number associated with the office. With this feature, a LATA can be associated with a subscriber. This assigned LATA number can be used to:

- select the appropriate signaling link based on the signaling transfer point (STP) for local area signaling services (LASS) services,
- populate the LATA value in the SSP 800 TCAP query to the service control point (SCP).

For additional information about LASS services see "Local Area Signaling Service Features," Section 11.10 in this document and refer to the 235-190-130, *Local Area Signaling Services* manual. For information about SSP 800 see "Service Switching Point 800 (SSP800) Number Service Feature," Section 11.8 in this document and 235-190-115, *Local and Toll System Features* manual.

This is a secured feature (SFID=171) and a right-to-use (RTU) fee must be paid to Lucent Technologies before enabling information is provided.

11.11.2 Background

The original design of the LASS and SSP 800 capabilities assumed (consistent with Bellcore requirements) that all lines served by one end office (EO) would reside in one LATA. LASS transaction capabilities application part (TCAP) queries from any line resulted in queries to the STP which corresponded to the LATA NUMBER field from the Office Options Form (item 56) and SSP 800 calls from any line resulted in queries to the service control point (SCP) database that included the LATA number from the same Office Options Form (item 56). Calls received over trunks were allowed to designate another LATA number based on the Trunk Group Form (FAR END LATA, item 116) (RC/V View 5.1).

SS7 traffic from a 5ESS®-2000 switch is sent via the host switch and the host sends traffic from multiple LATAs to a single STP pair. But, a local exchange carrier (LEC) STP pair was restricted to only serving callers within its own LATA. SSP 800 call queries use the same A-link regardless of the LATA but the TCAP query specifies the LATA of the originating subscriber.

11.11.3 Availability

This feature is distributed in the 5E11 software release.

11.11.4 Feature Environment

This feature is provided by office.

11.11.5 Feature Operation

This feature permits lines (or groups of lines) to be assigned a LATA number different from the default LATA number associated with the office. This assigned LATA number is used to select the appropriate signaling link and STP for LASS services based on a LATA and application. Or the assigned LATA number is used to populate the LATA values of the SSP 800 query.

A set of A-links can be built from the host to the LEC STP pairs in each LATA, so the host switch can differentiate which calls originate in a given LATA and send those calls to the appropriate LEC STP.

In processing a TCAP query, the Line Class Code (LCC) Form (RC/V View 4.1) derives the digit analysis selector (DAS) and Screening Index just as the Trunk Group Form does. Thus, the LATA associated with the subscriber is used during TCAP LASS query processing to determine the destination point code (DPC) for the query. The DPC corresponds to the appropriate STP for the TCAP LASS query. In processing SSP 800 calls, the LATA associated with the line (default is the office LATA) is used in the formulation of the TCAP query.

Originating LASS calls from lines in designated Rate Areas use the LCC value of the LATA NUMBER field for LASS TCAP queries to route to the STP for the line's LATA. In addition, originating SSP 800 database queries from lines will use the line's LATA in toll-free database queries and in any resulting AMA records. If no LATA number was specified on the LCC for a line, the LATA NUMBER field from item 56 of the Office Options Form 5509 (RC/V View 8.15, field 7) will be used.

This "TCAP Improvements for a Switch Spanning Multiple LATAs" feature affects TCAP processing only if the feature is active in the office.

11.11.6 User Operation

The service provider must unlock this secured feature and activate the feature using recent change procedures.

Only the switch administrator will use the new LATA NUMBER field, and then only when creating new classes of lines within Rate Areas outside the default LATA. When creating a new Line Class instance in a Rate Area outside the default LATA, the provider enters the LATA number associated with that Rate Area on the Line Class Code (LCC) Form (RC/V View 4.1). If no LATA number is entered, the LATA NUMBER field from the Office Options Form will be used for LASS TCAP query routing or in the formulation of 800 SSP queries.

Normal line/DN assignment procedures are unaffected by this feature.

To send TCAP traffic to different STPs based on the LATA/Application, the service provider specifies the pair of point codes associated with the LATA and application.

11.11.7 Engineering

11.11.7.1 Hardware Resources

No hardware considerations are associated with this feature.

11.11.7.2 Software Resources

No software considerations are associated with this feature.

11.11.7.3 Transition Considerations

There are no transition considerations associated with this feature.

11.11.8 Interactions and Limitations

This feature supports seven LATAs per application in addition to the one specified by the office form.

11.11.9 Incompatibilities

There are no incompatibilities associated with this feature.

11.11.10 Dependencies

This feature assumes that SSP 800 service and the following LASS services exist on the 5ESS®-2000 switch - automatic callback/automatic recall (AC/AR) and calling name delivery (CNAM).

11.11.11 Isolation Constraints

Not applicable.

11.11.12 Feature Implementation

11.11.12.1 Office Data Administration (ODA) Provisioning

There is no ODA provisioning associated with this feature.

11.11.12.2 Recent Change Provisioning

The service provider must unlock this secured feature and activate the feature using recent change views.

This feature assumes that SSP 800 service and the following LASS services exist on the 5ESS®-2000 switch - automatic callback/automatic recall (AC/AR) and calling name delivery (CNAM).

For additional information about LASS services see "Local Area Signaling Service Features," Section 11.10 in this document and refer to the 235-190-130, *Local Area Signaling Services* manual. For information about SSP 800 see "Service Switching Point 800 (SSP800) Number Service Feature," Section 11.8 in this document and 235-190-115, *Local and Toll System Features* manual.

Unlock the security lock for the feature by populating Recent Change View 8.22, *Secured Feature Upgrade*:

FIELD	VALUES
FEATURE ID	171
MODULE	(OFC or SM 1-192)
PASSWD	(Provided by Lucent Technologies SFID Administrator)
ACTIVE	Y

"Y" - Turns on (unlocks) the feature

"N" - Turns off (locks) the feature

Define the application type and assign destination point codes to a LATA using Recent Change View 8.17, *Direct Signaling Application*:

FIELD	VALUES
LATA	100-999 (Default=0 blank)
APPLIC	ACND or LASS
TRANS_TYPE	Translation type 0-255
DPC-1	Destination point code (9 characters)
DPC-2	Destination point code (9 characters)
SUB SYS NBR	subsystem number

Create a line class code (LCC) with the new LATA number using Recent Change View 4.1, *Line Class Code*:

FIELD	VALUES
LATA	100-999 (Default=0 blank)

Use other fields to create lines as needed.

* See 235-118-2xx, *Recent Change Reference* for detailed information on allowed values.

11.11.12.3 Customer Premises Equipment (CPE)

No CPE is required for this feature.

11.11.13 Maintenance Considerations

The **OP:LASSRQST** message has been modified to allow specification of a LATA for the LASS query. If no LATA is specified the office default LATA is used. See the 235-600-700, *Input Messages* and 235-600-750, *Output Messages* manuals.

11.11.14 Administration

11.11.14.1 Measurements

This feature does not impact measurements.

11.11.14.2 Billing

This feature does not impact billing.

11.12 FRACTIONAL DS1 SWITCHING VIA PRI (FRACTIONAL DS1/ISDN)

11.12.1 Definition

This feature offers customers a multibearer capability by switching multiple rates of 64 kbps (that is, Fractional DS1/ISDN). The N x DS0 switching will allow users to perform point-to-point application on a call-by-call basis by selecting the appropriate Customer Premises Equipment (CPE) supported transfer rate. Calls can be requested at speeds of 128 kbps to 1536 kbps, in 64 kbps increments. This feature supports circuit-switched calls.

The Fractional DS1 Switching via PRI (Fractional DS1/ISDN) feature combines the control and signaling access capabilities of PRI with the wide band switching capabilities of the SM.

NOTE: Refer to 235-190-104, *ISDN Feature Descriptions* for a complete description of this feature. The feature, as described in this document, is limited to the ISUP signaling protocol for wide band calls and basic capability of the feature as related to ISUP.

11.12.2 Availability

The Fractional DS1/ISDN feature is available with the 5E9(1) and later software releases.

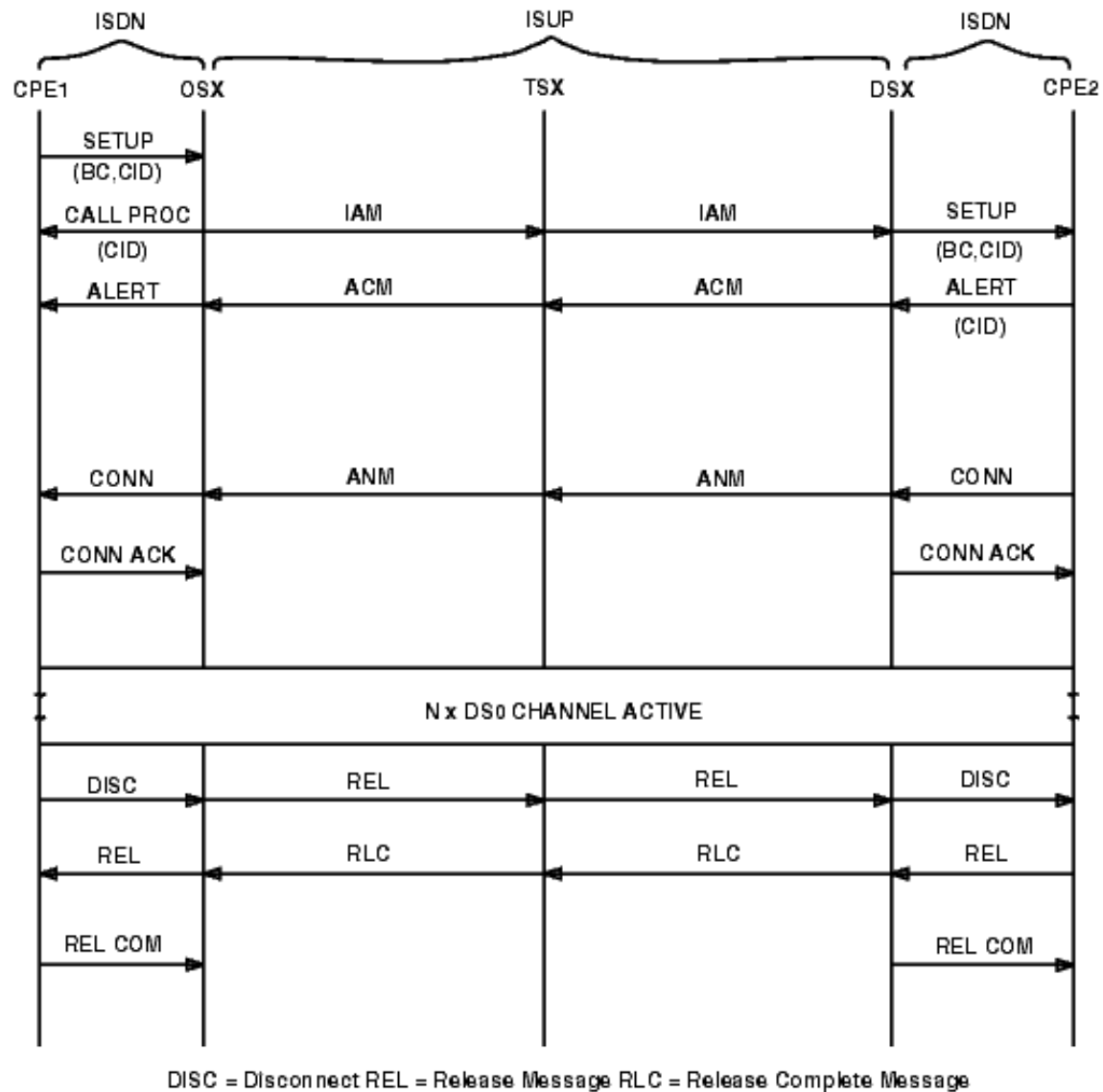
11.12.3 Call Processing Treatment

This section describes call processing treatment for Fractional DS1 calls. Call establishment and disconnect procedures are very similar to any ISDN circuit switched call except that extensions to Q.931 messages are needed to identify the data rate of the call and the B-channels on which the call is carried.

Figure 11.12-1 shows the call establishment message flow for a typical end-to-end wide band call. In the figure, CPE 1 is the originating end and CPE 2 represents the called party. The originating switch complex (OSX) receives a SETUP message from CPE 1.

The coding of the bearer capability (BC) information element (IE) identifies the call as wide band. The channel identification (CID) IE identifies the T1 facility on which the wide band call will be offered and the B-channels assigned to the call.

After receiving a SETUP message for a wide band call and determining how to handle the call, the OSX returns a CALL PROCEEDING message to CPE 1. Since the call is an interoffice call, the OSX also formulates an SS7 Initial Address Message (IAM) and codes the data rate and circuit identification code (CIC) for the controlling trunk in the User Service Information (USI) parameter. When the destination switch complex (DSX) receives the IAM, it formulates a SETUP message. The switch codes the BC IE with the transfer rate information and CID IE with the DS0 time slots selected. The bundle of DS0s at the CPE1-OSX and CPE2-DSX interfaces are selected independently. The rest of the setup and disconnect procedure is identical to that for any ISDN 64 kbps switched circuit-mode call.



DISC = Disconnect REL = Release Message RLC = Release Complete Message

OSX = Originating switch complex

IAM = Initial Address Message

BC = Bearer Capability Info Element

TSX = Tandem switch complex

ACM = Address Complete Message

CID = Channel Identification Info Element

DSX = Destination switch complex

ANM = Answer Message

Figure 11.12-1 N x DS0 Call Origination/Termination Scenario OSPS - CCS interface

11.13 OPERATOR SERVICES POSITION SYSTEM (OSPS)

11.13.1 CUSTOMER ACCOUNT SERVICES ENHANCEMENTS

Two parameters and one field have been added. The two IAM parameters are the Operator System Indicators parameter and the Generic Digits parameter, and the new field is the Sequence Call Indicator, which is bits OP of the Routing Information Indicator parameter.

The Operator System Indicators provide an Access Prefix Type Indicator and Handling Type Indicator that, together, convey whether the sequence call is handled 0+, 0-, or Automated. The allowed values for the Access Type Indicator are "0001 0001," "0001 0010," and "0001 0011," which indicate "1+," "0+," and "0-" access types, respectively. The allowed values for the Handling Type Indicator are "0010 0001," and "0010 0011," which indicate "manual station" and "automated station," respectively.

The Generic Digits parameter is used to carry the truncated and reformatted card number. It is coded as an "authorization code," with a value of "00001." The Sequence Call Indicator is used to convey whether the call is the "first call," "01," or a "subsequent call," "10" within the network.

11.13.2 OPERATOR SERVICES POSITION SYSTEM (OSPS) DESCRIPTION

The Operator Services Position System is a modern digital operator system providing a full range of operator services for directory assistance and toll and assistance (T&A) applications. It can be integrated into local, toll, local/toll, and tandem switches.

Available in the OSPS T&A application are automated calling features including automated calling card service, automated coin services, and operator assistance services. Provided also is the ability to originate and receive calls to and from other operator systems.

11.13.3 OSPS USE OF COMMON CHANNEL SIGNALING (CCS)

The toll and assistance features include the ability to bill calls to the following:

- Calling cards
- Third numbers
- Collect to called number
- Originating line number.

The CCS queries are sent to the billing validation databases to determine whether billing is acceptable. Card validation ability and acceptability of billing is provided for inward requests received from other operator systems.

The OSPS has the ability to validate CCITT and Commercial Credit cards automatically, using SS7 signaling for card validation. Consultative Committee on International Telephone and Telegraph (CCITT) format issued cards in foreign databases use CCITT SS7 signaling through a gateway Signaling Transfer Point - International (STPI) that provides access to the international credit card validation databases.

Database-related capabilities that are available in the OSPS include:

- Geographic Restriction and Purchase Limits
- Customer Defined Bill Segmentation (CDBS). CDBS is provided by international credit card verification (ICCV).
- Terminating Code Screening (TCS) Override.

Refer to Table 11.13-1 .

Table 11.13-1 OSPS Use of Common Channel Signaling

FEATURE	SIGNALING TYPE				DATA BASE Addressed ^a
	DCIS6	SS7			
		LEC	IEC	CCITT	
Billed Number Screening	X				BVA
Billed Number Screening		X			LIDB
Calling Card Verification	X				BVA
Calling Card Verification		X			LIDB
Calling Card Verification		X			BVD
Calling Card Verification		X			CAS
Calling Card Verification			X		CCC
Calling Card Verification			X		CAS
Calling Card Verification				X	ICCV
Network Call Denial	X				NCD
Subaccount Billing		X			LIDB
Terminating Code Screening Override			X		CAS
Customer Defined Bill Segmentation			X		CAS
Customer Defined Bill Segmentation				X	ICCV
Software Defined Network			X		CAS
Geographic Restrictions	X				CAS
Geographic Restrictions			X		CAS

Notes:

- a. The following are expansions of terms used in this table:

BVA = Billing Validation Application

BVD = Billing Validation Data Base (LIDB Compatible to validate CCITT format cards)

CAS = Customer Account Services

ICCV = International Calling Card Validation

LIDB = Line Information Data Base

NCD = Network Call Denial

11.13.4 OSPS CCS PROCESSING

11.13.4.1 Interface

The OSPS CCS processing provides the interface between the OSPS and CCS network databases for calling card service, billing number screening (BNS), and NCD. The OSPS CCS processing uses the DCIS6 and TCAP protocols to send messages to the CCS databases and receive replies.

11.13.4.2 Query Types

There are three types of CCS queries handled by the OSPS. These queries are as follows:

- **Calling Card Service Queries:** This query is sent to validate a calling card number and personal identification number that has been entered by a customer or an operator. The calling card service queries are sent to either a Line Information Database (LIDB), BVA, Customer Account Services databases, International databases, Commercial Credit Card data bases, or Billing Validation databases. Interexchange carrier issued CCITT format 89 cards are validated in the Billing Validation databases. Internationally issued CCITT format 89 cards accepted in this country are validated in foreign databases.

Recent change views are used to determine what database should be used to validate the card. The Card Recognition Table is first searched to see if the card is contained in the table. If so, the Card Attributes Table is used to determine the validation database. Tables 11.13-2 and 11.13-3 contain the recent change views used.

Table 11.13-2 Calling Card Recognition/Attributes - Recent Change Views

VIEW 8.9	VIEW 27.55	VIEW 27.56
CAS ON CCC ON CAS R3 ON	RLTCR_F2DV - RLTCR_F7DV Relations	RLCRD_ATTR Relation

Those cards not found in the Card Recognition Table are assumed to be LEC 10+4 cards, if the number is 14 digits in length. The LEC 10+4 cards use the following views to determine whether to validate in the BVA or LIDB.

Table 11.13-3 LEC Calling Card Service Validation - Recent Change Views

VIEW 8.9	VIEW 27.32 AND 27.33
ATT INTER LEC INTER ATT INTRA LEC INTRA DEFAULT	RLNPA_HEAD Relation RLNPA_NXX Relation

- **Billing Number Screening:** This query is sent to either the BVA or LIDB for verifying whether a directory number is allowed to be billed as a collect number or a third party number. The recent change views shown in Table 11.13-4 are used to determine which data base to send the queries for validation.

Table 11.13-4 Billing Number Screening Queries Validation: Recent Change Views

VIEW 8.9	VIEW 27.32 AND 27.33
ATT INTER LEC INTER ATT INTRA LEC INTRA DEFAULT	RLNPA_HEAD Relation RLNPA_NXX Relation

- **Network Call Denial:** This query is sent on calls that are not validated by the customer account services database to insure that the number being billed for the call is not delinquent in payment.

11.13.4.3 Query Timing Requirements

All OSPS query types require the replies to be received within a specified amount of time from the time the query is sent. This time is specified by the Telephone Company Administration using recent-changeable parameters. Each of the query types maintain separate timing parameters. The recommended time-out period for all types is 2 seconds. If a reply is not received within the specified amount of time, the calling process is informed. Any late or duplicate replies are ignored and are not returned to the calling process. To change any of these time-out values from the recommended value, the recent change views shown in Table 11.13-5 can be used. The time-out interval is recent-changeable on each attribute entry in the card recognition tables. This allows the owner to treat each card issuer individually even though they may use the same signaling.

Table 11.13-5 Changing Query Time-Out Values: Recent Change Views

QUERY	VIEW 8.9 FIELD NAME
BVA Calling Card	TIME
BVA BNS	TIME

NCD	TIME
LIDB Calling Card and BNS	CC AND BNS TIME
CAS (DCIS6)	TIME
QUERY	VIEW 27.56 FIELD NAME
CAS (CCS7) ICCV 89/CCC (ANS [®])	QUERY TIME-OUT

11.13.5 DATABASE INITIATED NETWORK MANAGEMENT CONTROLS

11.13.5.1 Customer Account Services And NCD Database Management Controls

For SS7, every customer account services reply, for which automatic call gapping (ACG) applies, contains network management information specifying the severity level of overload currently experienced by the database. Each reply contains two fields used for installing database-initiated ACG controls:

- The control level, which indicates the length of time that elapses between queries.
- The control duration, which indicates the length of time the control remains in effect.

If the control level in a customer account services reply is greater than 1, the ACG control is installed against the control address in use.

This control address is the first six digits of the individual account number [the individual account number follows the issuer identifier number (or 891IIN prefix)]. For Commercial Credit Cards (CCC), the fourth, fifth, and sixth digits of the card number are used.

If the control level in an NCD reply is greater than 0, an ACG control is installed against the control address. For NCD, the control address is the first three digits of the billing number (NPA or RAO).

The OSPS CAS SS7 and LIDB processing can maintain up to 256 simultaneous customer account services SS7 call gapping controls, 64 simultaneous NCD call gapping controls, 64 CAS CCS6 call gapping controls, and 256 LIDB call gapping controls.

When a customer account services or BVD database is overloaded, it includes call gapping control information in the TCAP reply. The OSPS CCS processing uses the gapping index and duration index to install call gapping controls.

Gapping controls are maintained separately for 89C cards and CCC. For 89C cards, controls are based on the first 12 digits of the card. Those 89C cards with the same first 9 digits and validated in the same NCP (Digits 10-12 help determine this) are grouped together. For CCC cards, controls are based on the first 6 digits. Those CCC cards with the same first 3 digits and validated in the same NCP (digits 3-6 help determine this) are grouped together. A total of 256 groupings of controls can be maintained simultaneously.

11.13.5.2 Billing Validation Application Network Management Controls

Every CCS6 reply from the BVA database contains a database overload indicator which specifies whether the database is experiencing an overload and the severeness of the overload. The overload level ranges from 0 to 7, where 0 indicates no overload and 7 is the highest level.

The OSPS CCS processing uses the overload indicator to set up a linear cutback of N/8 (where N is the overload level). This means that for every 8 query attempts, N of those query attempts are blocked. The overload level is tracked separately for each NPA and revenue account office (RAO) number. The recent-changeable parameters that specify the duration of the cutback control are found in recent change views shown in Table 11.13-6.

Table 11.13-6 Linear Cutback Control Duration: Recent Change Views

QUERY	VIEW 8.9
	FIELD NAME
BVA Calling Card	OVLDTIME
BVA BNS	OVLDTIME

11.13.5.3 LIDB Network Management Control

When an LIDB database is overloaded, it includes call gapping control information in the LIDB reply. Similar to customer account services and NCD, OSPS CCS processing uses the control level and duration value to install call gapping controls.

For LIDB, OSPS controls each database separately. The LIDB database is identified by the originating point code in the query reply. Six-digit controls (NPA-NXX and RAO-O/1XX) are used. All controls for a given NPA and LIDB combination are grouped together and similarly; RAO and LIDB combinations are grouped. Up to 64 such NPA-LIDB and RAO-LIDB combinations can be controlled simultaneously. Any number of NXX or O/1XX combinations within these groups can be controlled.

11.13.5.4 ICCV Database (Network) Management Controls

Currently, database controls are not supported by OSPS for ICCV queries due to expected low query volumes.

Network controls are installed based on receipt of a Unit Data Service (UDTS) Message containing a diagnostic of network congestion, network failure, subsystem congestion, or subsystem failure. These controls, when installed, will block all queries to a particular location for a period of 5 seconds.

For CCCs, all cards with the same sequence in digits 1-3 as the billing number in the returned query are affected.

For 89Cs using the customer account services TCAP message formats, all cards having the same sequence in digits 1-9 as the billing number in the returned query are affected.

Network controls are applied for ICCV according to the same guidelines used for customer account services TCAP.

Situations may arise when a particular query cannot be sent to the required database due to congestion or blockage in the CCS network. If this occurs, the network returns an abnormal reply and a network-initiated network management control is installed. For each query type, a network-initiated control blocks all query attempts for the control address for a period of five seconds. The control address is:

- Calling Card (BVA and LIDB) - First 3 digits of card
- BNS (BVA and LIDB) - First 3 digits of billing number
- NCD - First 3 digits of billing number
- Calling Card (DCIS6) - First 3 digits of account number
- 89C Card (Customer Account Services SS7 and BVD) - First 9 digits of card
- CCC Card (Customer Account Services SS7 and BVD) - First 3 digits of card
- 89C Card (ICCV) - First 9 digits of card

11.13.6 TEST QUERIES

Operator Services Position System provides test queries that are used along with event trapping to detect CCS network problems. Test queries are generated for Calling Card Service (BVA, LIDB, customer account services, and BVD), BNS (BVA and LIDB), and NCD. These test queries may be sent during any transition period. The test

input/output message (Im/Om) pages are shown in Table 11.13-7 .

Table 11.13-7 Test Queries Input/Output Messages

QUERY	INPUT MESSAGE	OUTPUT MESSAGE
BVA Calling Card Service	TST:CCRD	TST CCRD
LIDB Calling Card Service	TST:CCRD	TST LCCRD
BVA Billed Number Screening	TST:BNS	TST BNS
BVD 89/CCC ANS [®] TCAP Type 1	TST:AT1	TST AT1
LIDB Billed Number Screening	TST:BNS	TST LBNS
Network Call Denial	TST:NCD	TST NCD
Customer Account Services (DCIS6)	TST:CAS	TST CAS
Customer Account Services (SS7)	TST:CAS7	TST CAS7
ICCV	TST:ICCV	TST ICCV

11.13.7 EVENT TRAPPING

Event trapping requests the printing of messages when selected direct signaling events (DSEs) occur. Use event trapping along with test queries to monitor the quality of signaling traffic. Table 11.13-8 lists input/output messages for DSE trapping a variety of services such as, calling card service (CCRD), billing number screening (BNS) and network call denial (NCD). For a complete list of services and message format details see the 235-600-700, *Input Message Manual* and 235-600-750, *Output Message Manual*.

For information about event trapping with an Advanced Services Platform (ASP), see 235-190-125, *Advanced Services Platform Release 0 and 0.1A Feature Document* and 235-190-126, *Advanced Services Platform Release 0.1B Feature Document*.

Table 11.13-8 Event Trapping Input/Output Messages

MESSAGE TYPE	MESSAGE ID	DESCRIPTION
Input	SET:DSE	Request to turn on trapping for a DS event.
Input	CLR:DSE	Request to turn off trapping for a DS event.
Input	OP:ST-DSE	Request status (on/off) of a DS event.
Output	OP:ST-DSE	Reports status (on/off) of a DS event, requested by OP:ST-DSE.
Output	REPT:DSE	Reports status (on/off) of a DS event, such as INWATS or NCD.
Output	REPT:OSPS-DSE	Reports occurrence of an OSPS DS event.
Output	REPT:LN	Reports state of a new link node (LN).
Output	REPT:ACP-APP-SM	Reports occurrence of trapped event at an action control point (ACP).
Output	REPT:OSPS-ICE	This automatic report describes invalid combinations of data received from the CAS NCD in SS7 signs and messages.

11.13.8 OSPS QUERY MEASUREMENTS

Traffic measurements are the basic measurements for OSPS and provide a description of the performance of the system. The OSPS measurements relating to CCS query traffic tell how many queries were sent and how many replies were successfully received. These measurements also show how many queries were indeterminate (that is, due to time-outs, hardware problems, garbled responses, and not sent due to cutback). Refer to the following 30 minute traffic reports for various measurements.

- **SECTION 61 (OFA)** - Query attempts for each type of database.
- **SECTION 62 (OCCS)** - BVA and NCD Measurements
- **SECTION 109 (OATQ)** - LIDB and BVD Measurements
- **SECTION 110 (OCAS)** - Customer Account Services Measurements.
- **SECTION 135 (OCAS7)** - CAS7 Measurements.

In addition to the 30 minute traffic reports, following are some significant 24 hour plant measurement reports:

- **PART 12 (PT12)** - BVA and NCD Measurements
- **PART 17 (PT17)** - LIDB and BVD Measurements
- **PART 23 (PT23)** - Customer Account Services Measurements.

11.13.9 OSPS QUERY SOFTWARE ALARMS

Query software alarms provided for all query types are used to alert maintenance personnel of possible problems with the communications between OSPS and external databases over the CCS network.

At the end of each quarter-hour, the query traffic for that period is analyzed. If the percentage of successful queries falls below a defined threshold, an alarm is activated.

The query quarter-hour traffic is not analyzed and the alarm is reset for the following conditions:

- The CCS links are not operational.
- The number of query attempts for that quarter-hour has less than the minimum amount specified for the feature.
- The minimum amount specified is set to 0.

The following requirements apply to the alarm activation:

- When the percentage of successful rating queries fall below the defined threshold, and the alarm is not already activated, OSPS generates an alarm message to the 2SCCS computer. Alarms are activated at the Switching Control Center (SCC) and at the Master Control Center (MCC), and a query software alarm message is printed at both locations.
- If the alarm is already activated from another source, only the query software alarm message is printed at the SCC and MCC.

OM - REPT OSPS ALARM

Table 11.13-9 includes the recent change view global parameters for software alarms.

Table 11.13-9 Alarm Threshold Report: Recent Change View

QUERY	VIEW 8.9
	FIELD NAME
BVA Calling Card	MIN QUERY ALARM THR
BVA BNS	MIN QUERY ALARM THR
NCD	MIN QUERY ALARM THR
LIDB Calling Card	MIN QUERY ALARM THR
LIDB BNS	MIN QUERY ALARM THR
CAS (CCIS6)	MIN QUERY ALARM THR
CAS (SS7)	SS7 ALARM THR SS7 MIN QUERY
ICCV	ICCV ALARM THR ICCV MIN QUERY
BVD ANS/ [®] 89/CCC	MIN QUERY ALARM THR

11.13.10 RELEASE LINK FOR TOLL OFFICE

The Release Link for Toll Office feature (99-5E-4687) allows local toll service providers to use elements of the

generic Release To Pivot (RTP) procedure to provide release link ISUP trunks between a 5ESS®-2000 originating toll office switch and an operator system site. SS7 release link signaling using RTP permits the originating toll switch to release the trunk to the operator system switch (on a directory assistance call completion request) and reroute the call using information obtained from the operator system. This allows directory assistance call completion (DACC) calls to use non-dedicated SS7 trunks.

The Release Link for Toll Office feature also offers a release link directory assistance call completion service as specified by Nortel for the TOPS switch (Nortel's operator services switch), which uses non-standard signaling over dedicated SS7 trunks.

The Release Link for Toll Office feature is available in 5E14 and later software releases. For a full description, see 235-200-110, *Long Distance Platform Document*.

11.14 INTERSWITCH VOICE MESSAGE SERVICE

The Interswitch Voice Messaging Service (ISVM) feature allows VMS providers to expand their current intraswitch customer base to potential VMS customers served by other switches. As such, the main requirement of this feature is to provide switch support for the necessary interswitch signaling. This feature does not change or modify existing intraswitch VMS configurations, or their interface to the serving switch.

The ISVM feature is defined by the ability to provide VMS capabilities to a customer who may be served by a different switch than that connected to the VMS itself. The switch serving the VMS is referred to as the "near switch." If the VMS user is served by a different switch, that switch is referred to as the "far switch."

Figure 11.14-1 illustrates one possible architecture and includes the use of an intermediate tandem switch connected to a "far switch" and a "near switch." Such an intermediate tandem switch passes call forwarding parameters for ISVM to function. This figure indicates the switch, 1A ESSTM switch, and 4ESSTM switch software releases required.

NOTE: For more detailed information on the ISVM feature than is provided here, refer to the primary coverage in the Voice Features section of the 235-190-104, *ISDN Feature Descriptions* document.

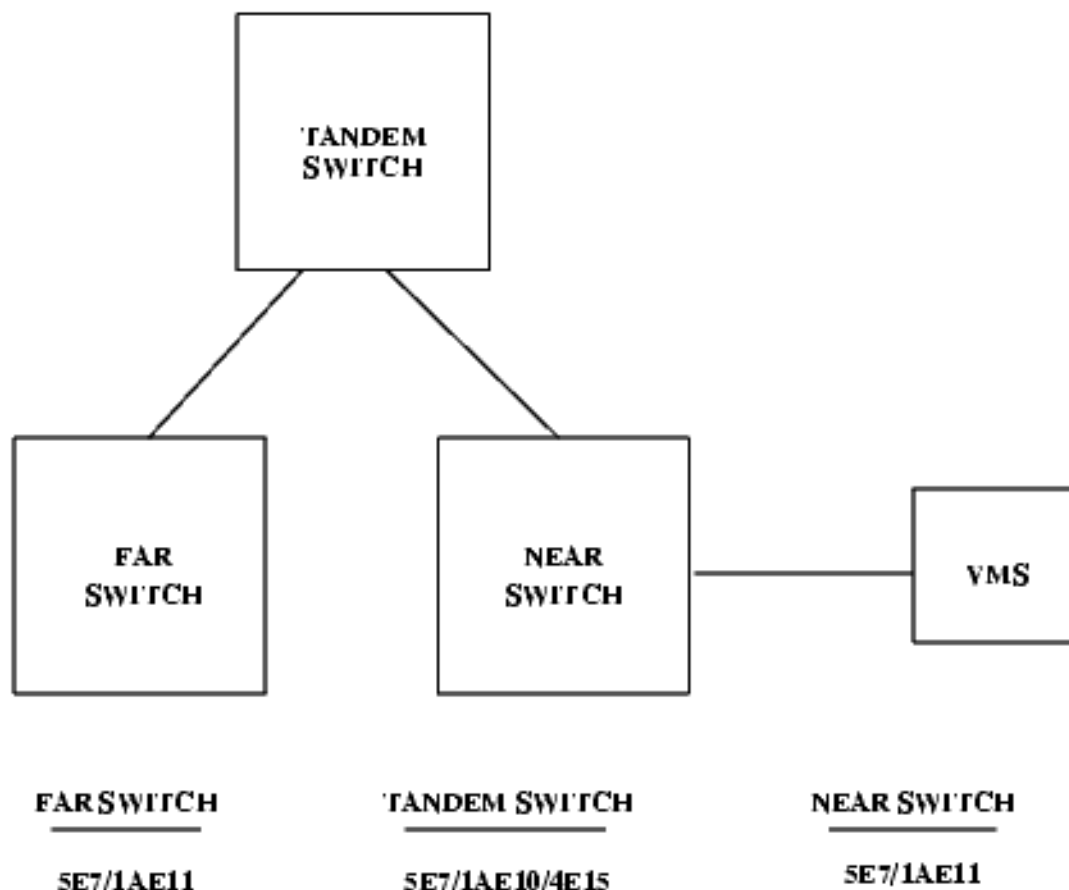


Figure 11.14-1 ISVM Switch Interface Configurations and Required Software Releases

11.14.1 Interactions

Messages that are transmitted on the switch/adjunct interface may be grouped into two categories: call history information (CHI) and message waiting indicator (MWI) control. The CHI is an incoming call-related message set

sent from the switch to the adjunct. The MWI control messages are exchanged between the adjunct and the switch to activate or deactivate an MWI at a user's station set, or to indicate that the switch cannot perform the MWI request.

The ISVM feature extends the existing message service center, CHI delivery, and MWI control functionalities to work across the switches. Transaction capabilities application part (TCAP) is the control protocol that is used for MWI. Also, working together with the ISDN User Part (ISUP) feature, the ISVM feature uses the new parameters: original called number (OCN), redirecting number (RGN), and redirection information (RI) (for example, the reason a forwarded call was forwarded— busy, no reply, or unconditional). The call control information is exchanged between the switch and the VMS system (or other adjunct).

With ISVM, the key is to be able to transmit data for these messages between switches. For this, the SS7 network is used. The VMS system is connected to a single switch, but serves a multiswitch area through use of the SS7 network.

The CHI information may or may not be sent through the toll network, but the 5E7 and later software releases can send and accept CHI parameters at the boundaries of the LEC network. The 5E8 and earlier software release toll switches discard CHI parameters at network boundaries.

11.14.2 Special Planning Considerations

The ISVM feature is an interswitch, intra-LATA service that is configured as such to operate properly. If it is not, unsuccessful operation results.

The service provider installs the SS7 signaling facilities that satisfy two conditions as follows:

- (1) Calls forwarded from any far switch to the near switch is routed entirely over trunks with SS7 signaling. Furthermore, the SS7 signaling protocol supports the call forwarding parameters needed for the CHI sent by the near switch to the VMS system.
- (2) The near and far switches support the SS7 messages used to send the specific interswitch MWI activate/deactivate messages.

The current and planned capabilities of the switch do not allow selectively routing calls over SS7 trunks. When calls are forwarded over non-SS7 trunks, the ISVM feature does not function properly.

11.14.2.1 SS7 ISUP Protocol

For every SS7 interswitch call, information required for call processing and service logic is carried between switches in an ISUP initial address message (IAM).

11.14.2.1.1 Setting the Mandatory ISUP Parameters for the Initial Address Message

Every IAM contains six mandatory ISUP parameters. These include the message type, nature of connection indicators, forward call indicators, calling party's category, user service information, and called party number (CdPN) parameters. In addition, an IAM may contain one or more optional ISUP parameters.

Refer to "Optional ISUP Parameters," Section 11.5.1 of this manual for the parameters that drive the service.

11.14.2.2 SS7 TCAP Protocol

For VMS, there are two TCAP messages that can arrive at a subscriber's switch which specify the activation or deactivation of a subscriber's Message Waiting Indicator (MWI). If the subscriber is an ISDN user, these TCAP messages must be mapped into Q.931 messages by the MSS feature. The MWI activation and deactivation

requests are mapped into the Q.931 "feature indication information element" and are included in an information message or any Q.931 call control message.

11.14.2.2.1 Message Waiting Indicator

The MWI alerts the VMS subscriber that a voice message is available for retrieval. This indicator can be either a visual lamp or a stutter dial tone, depending on the CPE. When the VMS subscriber and the VMS provider are situated on different switches, the near switch must send TCAP query messages to notify the far switch that a voice message is available or that a voice message is no longer available. See Figure 11.14-1 for definitions used in this section.

11.14.2.2.2 SS7 SCCP Procedures

The MWI TCAP query messages will be sent in the data field of an SCCP unit data message. Query messages will be routed via global title translation (GTT). Therefore, the destination point code (DPC) will be that of the STP doing the GTT. The originating point code (OPC) will be that of the near switch. The Protocol Class will be connectionless (class 0) and the Unit Data Service Option will be "return on error." The Called Party Address will contain a subsystem number of 0, a translation type for ISVM and a global title of NPA-NXX-XXXX, the 10 digit DN of the ISVM subscriber. The Calling Party Address will contain the subsystem number for ISVM and the point code of the near switch.

The MWI TCAP response messages will be sent in the data field of an SCCP unit data message. Response messages will be routed via DPC. The DPC will be that of the near switch and the OPC will be that of the subscriber's switch. As with query messages, the Protocol Class will be connectionless (class = 0). The Unit Data Service Option will be "return on error." The Called Party Address parameter will contain the subsystem number of the ISVM feature from the Calling Party Address parameter received in the initial message. Note the SSN for ISVM in called party address need not be the same as the SSN for ISVM in the calling party address.

11.14.2.2.2.1 Errors

The SS7 SCCP messages have a CNI header for transport on the CNI ring. The return bit is set in the CNI header for MWI activate/deactivate TCAP messages. The CNI returns the message if a problem in routing an outgoing message occurs (for example, congestion, subsystem number not defined, etc). Errors caused by returned messages are mapped to the error cause "blocked" in a failure message sent to the VMS system.

11.14.2.2.3 Message Available/Provided (MWI Activation/Deactivation)

The following describes the sequence of TCAP messages exchanged between near and far switches when a voice message is available or when all voice messages have been retrieved.

11.14.2.2.3.1 Send Notification from Near (VMS) Switch

When the Voice Message System informs its host switch that it has a message for a VMS subscriber or that all messages have been retrieved, the near switch must determine if the subscriber is supported by a different switch. If the subscriber is not, then the switch will follow the procedures for intraswitch MWI activation/deactivation which do not use TCP.

If the subscriber is served by a different switch, then a TCAP message must be sent using global title translation based on the subscriber's DN, to notify the served user that they have a voice message available or that all messages have been retrieved. Timer T(1) will be started with a default value of 3 seconds. It may have a value between 1 and 10 seconds. Also, some information provided by the VMS is stored in a temporary buffer at the near switch. This information may later be incorporated into an fail message sent to the VMS if a TCAP response message is received indicating that the activation or deactivation of a user's MWI has failed.

The notification message will be of the "Query with Permission" package type and will contain a single "Invoke

(Last)" component with an operation type of "Report Event - Voice Message Available" or "Report Event - Voice Messages Retrieved." The component will contain an "Invoke Identifier." There will be two "Digits" parameters contained within this component. The first contains the destination number (number of the served user), and the second contains the VM Storage and Retrieval ID (VMSR ID). The VMSR ID is generated by the VM switch and will be a number which uniquely identifies the VMS in the network. For this implementation of ISVM, a default value for VMSR ID will have all digits coded as 0.

The far (serving) switch may receive (from another vendor's switch) a VMSR ID parameter coded nonzero. This will cause no special action to be taken by the far switch.

11.14.2.2.3.2 Limitations

For this first offering of ISVM, the optional TCAP parameters "Time Stamp," "Calling Party Number," and "MWI Type" are not implemented; if they are received from another vendor's switch, they will be ignored. If in a future enhancement these parameters are supported, it is in this "Query with Permission" package that they will be included. The Time Stamp parameter gives the time and date the VMS received the message. The Calling Number gives the DN of the party who left the message. The MWI Type parameter is used to indicate a level of priority for the message.

If these optional parameters are received in a TCAP message, they will be ignored. However, the message format will be verified for TCAP correctness.

11.14.2.2.3.3 SEND RESPONSE from Far (Serving) Switch

Upon receiving the TCAP Query activation/deactivation notification, the far switch will notify the VMS user through the subscribed form of notification (lamp or dial tone). In normal situations, the far switch will serve the destination number and will be able to notify the served user that there is a voice message waiting, or that all messages have been retrieved by activating or deactivating their MWI indicator. To confirm success, the far switch will send a TCAP message of the "Response" package type containing a single empty "Return Result (Last)" component to the VMS switch. No parameters are present in this message.

If the activation/deactivation notification could not be performed, the far switch will send a TCAP message of the "Response" package type containing a "Return Error" component and error code to the VMS switch. The following service specific errors may be encountered and will be mapped to the cause, in parenthesis, in messages sent to the VM system:

- If the Destination DN is not currently assigned to an active interface, the far switch will return the error code "Unassigned DN (INV -invalid)."
- If the received Destination DN is not a 10-digit DN, the far switch will return the error code "Unassigned DN (INV-invalid)"
- If the far switch is overloaded and cannot currently handle the request, the far switch will return the error code "Task Refused (BLK-blocked)."
- If at the far switch, there is no feature in the destination DN's line data that has the security option set to "no" (that is, the destination DN is not a ISVM subscriber), then the switch will return the error code "Unassigned DN."
- If the far switch detects other TCAP data errors (for example, unavailable resources, and unexpected data value), the switch will return an appropriate error code in the TCAP protocol specification.

If the far switch receives a TCAP message with a missing mandatory parameter (Destination DN or VMSR Identifier), a Response package containing a "Reject" component will be returned to the near switch. If a far switch

receives a TCAP message with any unrecognized mandatory or optional parameter, a Response package containing a "Reject" component and problem code will be returned to the near switch. In either case, MWI activation/deactivation will not be carried out by ISVM service.

If other TCAP protocol errors are detected (for example, a message type, component type, operation code, or legitimate TCAP parameters other than those permitted for ISVM), a "Reject" component and problem code will be returned to the near switch.

11.14.2.2.3.4 Receive Response at Near (VM) Switch

If, after sending a Query message indicating Voice Message Available/Retrieved, the near switch receives a "Response" package containing a "Return Result (Last)" component, the near switch will cancel the waiting T(1) timer, discard the temporary buffer and its information, and assume that the transaction was completed. No corresponding message will be sent to the VMS.

If, after sending a Query message indicating Voice Message Available/Retrieved, the near switch receives a "Response" package containing a "Return Error" component, the near switch will cancel the waiting T(1) timer and generate an MWI_Fail message. This MWI_Fail message will be generated from the information received in the "Return Error" component, the error code, and the information in the temporary buffer. The MWI_Fail message is sent to the VMS and the temporary buffer is discarded.

If the waiting T(1) timer expires, an MWI_Fail message will be generated and the corresponding VM system-related information stored in TCAP will be deleted. Moreover, if a response is received after a time-out, then no additional MWI_Fail will be generated. However, if the late response was a return error or reject, then TCAP will trap this event.

Any TCAP error code other than the four specified for ISVM (that is, unavailable resources) will be mapped to the "blocked" error cause in the MWI_Fail message sent to the VMS.

If, after sending a Query message indicating Voice Message Available/Retrieved, the near switch receives a "Response" package containing a "Reject" component, the near switch will cancel the waiting T(1) timer and generate an MWI_Fail message. The problem code contained in the returned "Reject" component will be mapped to the "blocked" error cause in the MWI_Fail message sent to the VMS.

If a Confirm or a Fail message is not returned to the near switch before the T(1) timer expires, the notification attempt will be abandoned, and an MWI_Fail message with an error code of "blocked" will be sent to the VMS.

If a protocol or application error is detected by the near switch in the received Response message from the far switch, the near switch will cancel the T(1) timer and will send a Unidirectional Package containing a Reject Component or a Return Error Component, respectively, to the far switch. The near switch will also send an MWI_Fail message containing an "invalid" error code to the VMS. This unidirectional message will be discarded by the far switch.

11.14.2.2.4 Network Returned Messages

After sending a query or response message into the SS7 network, the message may be undeliverable to the final destination for a variety of reasons. Because the UDS option will be set in the SCCP header for both queries and responses, the SS7 network will return the message to the sender in these cases.

The message format will be identical to that sent with the exception of appropriate returned bits being set.

In the case of returned queries, the switch should notify the VMS of the failure, providing the appropriate error code mapped from that received in the returned query.

In the case of returned responses, the switch will not attempt to notify the VMS if no recovery is possible.

11.15 *AUTOPLEX*[®] CELLULAR TELECOMMUNICATIONS INTERWORKING TO SS7 ISUP SIGNALING

11.15.1 Definition

The switch *AUTOPLEX*[®] Cellular Telecommunications System Interworking feature allows a switch to be used to handle switching and other functions for cellular telephone systems. The changes necessary are all handled by the switch Digital Cellular Switch (DCS) and the Executive Control Processor (ECP), making this feature transparent to systems/networks on both sides of the interface.

The term Wireless Origination is a generic term that includes all calls where the Mobile Switching Center (MSC) is the origination side of the call (that is, mobile originations or the origination of the forward-to-leg for call forwarding). Wireless Termination is also a generic term which includes all calls where the MSC is the termination side of the call (that is, mobile terminations or the first leg of call forwarding).

11.15.2 Background

The switch *AUTOPLEX*[®] Cellular Telecommunications System product provides the basis for the next generation DCS for *AUTOPLEX*[®] Cellular Telecommunications System applications. This feature uses existing switch hardware and software in conjunction with the ECP complex from the current *AUTOPLEX*[®] Cellular Telecommunications System 1000 (APX-1000). The major change is the substitution of the switch for switching and other functions currently performed by the *DEFINITY*[®] G2 DCS. This allows higher system capacities in future releases. Also, the switch will coexist in an APX-1000 with local and remote *DEFINITY*[®] G2 DCSs. The functionally distributed architecture of the switch allows modular growth as well as providing duplicated hardware for reliability. Figure 11.15-1 provides an overview of the *AUTOPLEX*[®] architecture.

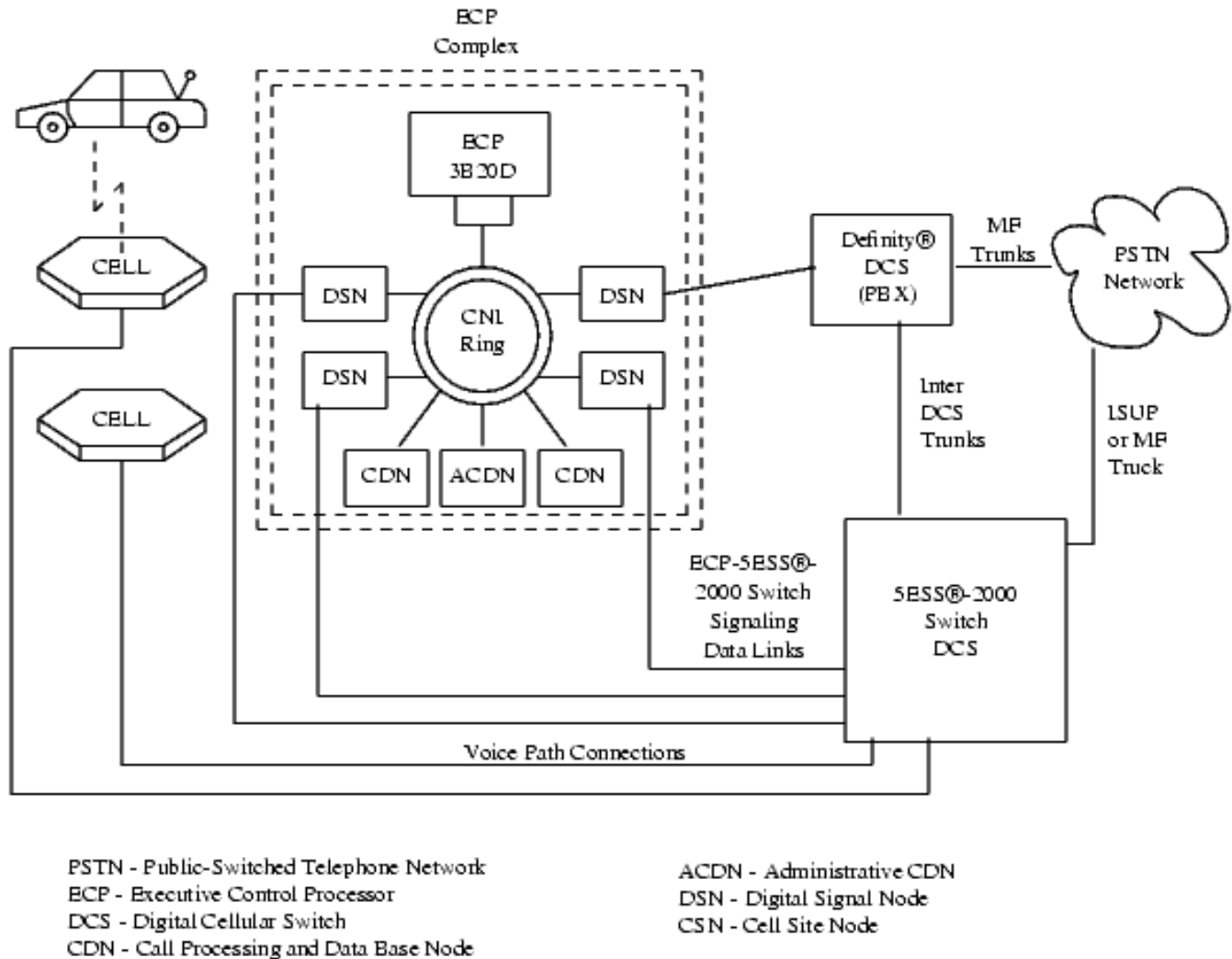


Figure 11.15-1 AMPS Overview

In addition to providing an initial cellular application, the switch AMPS feature also provides a basic platform for evolution to Personal Communication Services.

In the future, the switch will support the baselined APX-1000 Code Division Multiple Access (CDMA) system architecture and provide all switch specific hardware and software. A phased approach for CDMA will provide transition between phases by employing a graceful upgrade strategy (that is, transitions only require addition of new hardware and software capabilities, they do not interrupt services, and they do not require removal of equipment previously installed.)

The switch provides a trunk interface to the following:

- Radio Cell sites
- Public-Switched Telephone Network (PSTN)
- Other AMPS Mobile Telephone Switching Offices (MTSOs)
- DCS(s) on the same AMPS MTSO.

11.15.3 Partitioning Functionality Between ECP Complex And 5ESS®-2000 Switch DCS

Wireless call processing decisions are made by the ECP Complex. Therefore, port status data for all trunks are kept in the ECP. Billing records are generated by the ECP Complex, not by the switch DCS. The ECP Complex is the overall processor in the *AUTOPLEX*®-1000 Cellular Telecommunications System. Incoming ISUP7 signals on PSTN trunks are interworked to messages on the ECP switch signaling data links. Whatever information is received by the switch DCS is forwarded to the ECP Complex. Similarly, messages received on the ECP switch data links are interworked to ISUP messages and sent, via CN1 and STP, to the far switch.

The ECP complex does cell site trunk hunting, provides trunk group selection lists (TGSL) for network trunks, and provides instructions for connecting trunks. The switch software selects a network trunk to be used by a call using the ECP provided TGSL.

There is no subscriber data on the switch. In addition, mobility management in the form of location update, authentication, roamers support, etc. is handled by the ECP complex. The ECP complex gets instructions from the cell sites and the mobile station, and instructs the switch to take the appropriate action via data link message sets.

The ECP controlling philosophy is seen in how certain office data, populated by switch RC/V is not used by the software; instead corresponding data in the ECP complex provides similar functionality. The office data items shown in Table 11.15-1 are ignored in the switch DCS when cellular-originated calls are processed.

Table 11.15-1 5ESS®-2000 Switch DCS Ignored Items

VIEW NUMBER AND FIELD NAME	COMMENT
5.1 RCD 3PT1 ITC	Calls from ECPC not recoded Msg content determined by ECPC All NM operations applied in ECP
5.1 SS7 TYPE	
5.1 CONTROL TYP	
8.15 BUSY ANNC	
8.15 LEC ANNC	
8.15 LEC IW ANNC	
8.15 NI ANNC	
8.15 NI IW ANNC	Calls from ECPC not recoded Send CPN if ECPC provides it Send CHG if ECPC provides it Send CSI if ECPC provides it Value determined in ECP data ATP never sent from ECP UUI never sent from ECP
8.15 RCD 3PT1 ITC	
10.2 CPN SUBSC	
10.2 ANI IND	
10.2 CSI SUBSC	
10.2 CKT CODE	
10.2 ATP SUBSC	
10.2 UUI SUBSC	
Notes:	
a. These RC/V fields only apply to call failures that occur within the DCS. If a call failure is detected by the ECPC and the call is released back to the 5ESS®-2000 switch DCS, this indicator will not be used to determine whether a tone/announcement should be played or a whether a REL should be sent.	

11.15.4 Availability

This is a Secured Feature and is available with the 5E9(1) and later software releases. Because this is a secured feature it will not be enabled until the purchaser has made the necessary arrangements with Lucent Technologies. Information on feature enabling is provided upon ordering. Please contact your Lucent Technologies Network Systems Account Representative for ordering information and Right-to-Use (RTU) fee associated with this feature.

11.15.5 Network Configurations For A DCS Switch

The description in "Switching Offices," Section 10.2.2 defines switching offices that can be involved in ISUP network interconnect. Special considerations are needed for ISUP network interconnect as it relates to a DCS switch. The DCS switch is considered an end-office and can originate calls toward a carrier or terminate calls from a

carrier. Equal access calls that go out on ISUP trunks toward a carrier must either go directly to the carrier or go to an access tandem switch and then be switched to the carrier. Only one access tandem switch may be routed through before accessing a toll office.

Figures 11.15-2 and 11.15-3 provide a detailed illustration of a switch DCS originating and terminating end-office, respectively.

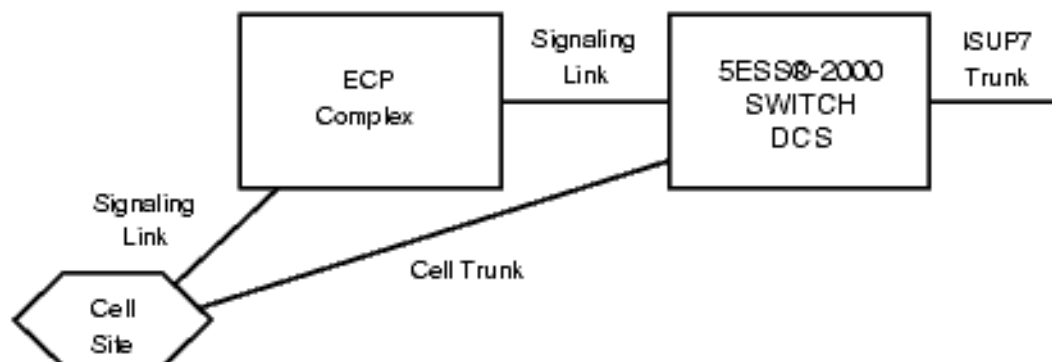


Figure 11.15-2 Switch AMPS Interworking to ISUP7 Originating Switch DCS Office

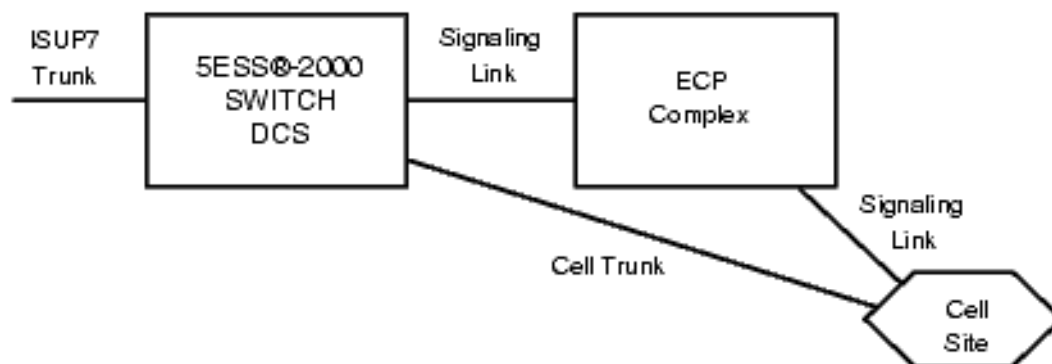


Figure 11.15-3 Switch AMPS Interworking to ISUP7 Terminating Switch DCS Office

11.15.6 ECP/DCS Signaling Messages

To support switch based SS7, the switch AMPS feature uses a set of ECP/DCS signaling messages that include parameters to support interworking between SS7 trunk signaling on the switch and AMPS call processing on the ECPC. The coding of the ECP/DCS SS7 parameters is very similar to the coding of ISUP parameters.

Messages received on the ECP switch signaling data links use SCCP subsystem 235. This subsystem number must be populated on view 8.17 to drive the correct processing of messages to/from the ECP Complex.

11.15.6.1 Parameter Mapping

This section describes the mapping between the ISUP messages that the switch receives/sends and the corresponding ECP/DCS messages. The messages are shown in Tables 11.15-2 and 11.15-3.

Table 11.15-2 Mapping From ECPC To ISUP Signals

INPUT FROM ECPC	ISUP SIGNAL
SETUP_S7X Called Party Number - Mandatory Calling Party Category - Mandatory	IAM

Forward Call Indicator - Mandatory Calling Party Number - Optional Carrier Selection Info - Optional Charge Number - Optional Original Called Number - Optional Originating Line Info - Optional Redirecting Number - Optional Redirection Info - Optional Transit Network Selection - Optional	
ANC_SETUP_S7X Same Parameters as SETUP S7X	IAM
ACM_S7X Backward Call Indicator - Mandatory Cause Indicators - Optional Optional Backward Call Indicators - Optional Automatic Congestion Control Level - Optional Redirection Info - Optional	ACM
CPG_S7X Event Info - Mandatory Redirection Number - Optional	CPG
ACPT_X No Parameters	ANM
ACPTWT_X No Parameters	ANM
COLLDIG_X No Parameters	ANM
CLEAR_X (orig) Cause Indicators - Mandatory Automatic Congestion Control Level - Optional	REL
CLEAR_X (term after ACM) Cause Indicators - Mandatory Automatic Congestion Control Level - Optional	REL
CLEAR_X (term before ACM) Cause Indicators - Mandatory Automatic Congestion Control Level - Optional	REL
MGinterrupt ^a (orig) No Parameters	REL
MGinterrupt ^a (term before ACM) No Parameters	REL
MGinterrupt ^a (term after ACM) No Parameters	REL
Notes: a. MGinterrupt is received by the 5ESS [®] -2000 switch DCS software when the ECPC sends a CLRCPM_X, RESET_X or STRES X message.	

Table 11.15-3 Mapping From ISUP Signal To ECPC Message

ISUP SIGNAL	OUTPUT TO ECPC
IAM	INCALL_S7X Forward Call Indicator - Mandatory Calling Party Category - Mandatory Called Party Number - Mandatory Calling Party Number - Optional Charge Number - Optional Original Called Number - Optional Originating Line Info - Optional Redirecting Number - Optional Redirection Info - Optional
ACM	CONNACK_X Backward Call Indicator - Mandatory Cause Indicators - Optional Opt Bw Call Indicators - Optional Automatic Congestion Cont - Optional Redirection Info - Optional
ANM	ANSWER_X Backward Call Indicator -Optional
SUS	DISC_X No Parameters
RES	ANSWER_X

	Backward Call Indicator - Optional
CPG	CPG_S7X Event Info - Mandatory Cause Indicators - Optional Redirection Number - Optional
REL	DISC_X Cause Indicators - Mandatory Automatic Congestion Cont - Optional
REL	DISC_X Cause Indicators - Mandatory Automatic Congestion Cont - Optional
RSC/GRS	FAIL_X (for RSC, GRS) No Parameters
BLO/CGB	FAIL_X (for BLO, CGB) No Parameters
EXM	EXM_S7X Outgoing Trunk Group - Optional

The switch is responsible for generating the user service information parameter in the IAM message. For cellular-originated calls, the switch DCS will always set the information transfer capability to 3.1 kHz audio.

The following are general rules of call processing for switch based SS7:

- For incoming calls, the voice path assurance test procedures are handled completely by the switch DCS, before an INCALL_S7X message is sent to the ECPC.
- The SETUP_S7X message is used for routing equal access calls (that is, to IECs) as well, and include additional SS7 parameters to pass the appropriate information, such as carrier selection and charge number.
- Unrecognized ECP/DCS SS7 parameter codes are ignored.
- When the switch DCS receives the ISUP Release (REL) message, it will forward the appropriate cause (that is, user busy) to the ECPC in the DISC_X message. The ECPC is responsible for requesting the appropriate tone or announcement by sending a TONERREQ_X/ANCREQ_X/E_TONERREQ_X message to the switch DCS.

For Wireless Terminations, when the switch receives the IAM message, it passes the parameters to the ECPC via the INCALL_S7X message.

11.15.6.2 Call Clearing

For Wireless Initiated Clearing (that is, Mobile Unit Release), the ECPC sends the CLEAR_X message; this gets mapped to a REL message.

For PSTN Initiated Clearing (that is, land line on-hook), when the switch receives the REL message, it passes a DISC_X message to the ECPC. DISC_X can also result from a SUSpend message. To distinguish the two cases, a SUSPND bit is populated in the DISC_X message. A value of 1 is a signal that the ECPC should not perform reanswer timing. A value of 0, along with the fact that the called telephone was analog, triggers a timed release disconnect timer to be set in the ECPC.

As a safety net for timed release disconnect timing in the ECPC, another timer is set in the switch DCS software. When the switch DCS originating end office gets a SUSpend message and the called party is an analog phone, a timed release disconnect timer is started. The value used for this timer in the switch DCS software is APX DAT + 2 seconds. APX DAT is a disconnect acknowledge timer used for communication to the ECPC and has a range of 5-25 sec. The primary timed release disconnect timer in the ECPC has a smaller value and will fire first.

11.15.7 SS7 Engineering

The switch (serving as DCS) terminates the SS7 data links from the ECP on the administrative module (AM) via a CNI ring.

The switch and ECP are network elements with unique point codes. The interface message set between the switch and ECP are "encapsulated" in SCCP Class 1 connectionless protocol. The data links between the switch and ECP are nonencrypted.

The switch and ECP communicate via an associated signaling relation on a single link set. This link set is the primary and only signaling route between the switch and ECP.

The ECP switch signaling data link set is engineered with a minimum of two links for reliability. Up to a maximum of eight links are supported in the link set. The links are diversely routed for reliability.

The single link set connecting the switch and the ECP is a point-to-point link connection, terminating at link nodes on both the *AUTOPLEX*® Cellular Telecommunications System CNI ring and the switch CNI ring. The switch and ECP serve as Service Entry Points (SEP). The links connecting the SEPs are known as "F links" in the Bellcore TR-NWT-000246 Specification. However, the ECP switch signaling data link is engineered and provisioned on the switch as NO STP.

Messages arriving from the ECP at the switch CNI ring are split off to route them to either the AM or CMP, or directly to the appropriate SM. Messages from the switch to the ECP are sent directly from the DLN using the point code destination and subsystem number of the *AUTOPLEX*® Cellular Telecommunications System and Signaling Link Selection (SLS) field assigned.

The ECP switch links use V.35 protocol and operate at 56 kb/s. When the switch and ECP switch are co-located, a data set is used at each end. For longer distances on these links a D4 channel bank and T-carrier can be used.

The ECP switch links operate at 56 kb/s (clear).

The switch CNI ring terminates PSTN related A-links, terminating at network Signaling Transfer Points (STPs), for PSTN SS7 and TCAP traffic. The links connecting an STP and SEP are known as "A links" in the Bellcore TR-NWT-000246 Specification.

Existing PSTN connections requiring SS7 signaling (ISUP7) are also supported at the switch.

11.16 CENTREX NETWORK

CENTREX Network (CN) consists of three service offerings or features:

- CN itself,
- CENTREX Network -- Special/CENTREX Network-Government (CN-S/CN-G), and
- CENTREX Network -- Interswitch Voice Mail (CN-ISVM).

All three of these are secured features. CN must be active when either CN-S or CN-ISVM is active.

CN provides the ability to extend a Switch CENTREX Group or Terminal Group and its intraswitch functionalities across a set of switches by use of the Business Group parameter within the SS7 signaling. CN expands the notion of a single switch business group (terminal group) and its functionalities to a Multiswitch Business Group (MBG). Thus, a business group consisting of many geographical locations, each being served by one of the CN switches, can define one CENTREX group for all of its business group locations.

This manual describes the SS7 impact of the CENTREX Network feature. For more detailed information on CENTREX Network, see 235-190-103, *Business And Residence Feature Descriptions*.

CN can be used in an intra-LATA network that includes tandem switches. When receiving an MBG call, a tandem switch should pass all unrecognized parameters through, with no processing of the Business Group parameter being done at the tandem switch. (However, please note the difference for tandem switches in a CN-S/CN-G network. See Section 11.16.1, "CENTREX Network - Special/Government [CN-S/CN-G] Feature.")

When used as a tandem within a CN network, the switch will operate as previously described. When another type of switch is used as a Tandem, it should operate as previously described, but the service provider should verify this when setting up their MBG network.

11.16.1 CENTREX Network - Special/Government (CN-S/CN-G) Feature

A CN-S/CN-G network allows Tandem switches within its intra-LATA network, but these tandems must populate MBG data so as to be able to recognize and process incoming MBG calls. Currently, the switch is the only switch able to support the Tandem switch operation required for CN-S/CN-G. Therefore, CN-S/CN-G networks can only be set up in networks without Tandems, or where all Tandems concerned are switches.

Also, unlike a CN network, a CN-S/CN-G network has dedicated MBGID marked SS7 trunks to service its MBG calls and SFG control of MBG call overflow from these trunks onto the SS7 public trunking network. Marking the CN-S/CN-G SS7 trunks with an MBGID prevents CN-S/CN-G-network-specific information from leaving the CN-S/CN-G network, as network-specific information is only allowed to be transported on these marked SS7 trunks. An MBG call routed to an SS7 trunk that is marked with a different MBGID than the MBG call will still be allowed transport on the marked SS7 trunk. Only network-specific information is prevented from being passed in this case.

11.16.2 DSN/AUTOVON Precedence Call Handling

When a Defense Switched Network/Automatic Voice Network (DSN/AUTOVON) call enters the multiswitch CENTREX Network and is forwarded over CCS7 trunks to the ISDN attendant, the DSN/AUTOVON identity, as well as its precedence level, is retained and is presented to the attendant. Message-Level Precedence and Preemption (MLPP) features can be provided, if available on each end of an interswitch trunk.

11.16.3 External Network FX, TIE, And FTS-2000 Call Handling

This capability allows other trunk calls entering the multiswitch CENTREX network to retain their identity: FX, TIE, or

FTS-2000. This identity, passed in the ISUP Generic Digits parameter, is established from the incoming trunk type for the trunk entering the multiswitch CENTREX network. When such calls are forwarded over the multiswitch CENTREX network's CCS7 network (dedicated to CN-S traffic only) to the centralized attendants, the forwarding switch will place information in the ISUP message to identify the incoming trunk type. This information is then delivered to the attendant for display. For forwarded calls, the attendant will receive this trunk identification information (and precedence information if a DSN trunk) in addition to the reason for forwarding.

11.16.4 CENTREX Network - Interswitch Voice Mail (CN-ISVM) Feature

CN-ISVM cannot be offered unless the basic CN feature is also offered. For a given MBG, CN-ISVM adds the ability to offer a centralized screened Voice Mail Service (VMS) for the members of the MBG to the CN functionality.

"Screening" means checking the Business Customer ID (BCID) of the station forwarding the call to make sure it is a paying VMS customer, by calling directly to the VMS. The BCID is made available on the near switch (switch serving the VMS) for interswitch calls because the received MBGID or MBGIDs can be translated into a BCID or BCIDs.

When an MBGID is defined on a switch, the MBGID can also be mapped to one BCID (one at most, although many MBGIDs can map to the same BCID on a switch), and the BCID to which the MBGID is mapped must be defined and supported by the MSS group to which the MBG belongs.

For example, on a given switch, MBGID 10 may be mapped to BCID 4, and MBGID 11 may also be mapped to BCID 4. MBGID 10 is served by MSS group 1, for which BCID 4 is defined and supported, and MBGID 11 is served by MSS group 2, for which BCID 4 is also defined and supported.

The switch administration personnel must make sure these relationships are correctly defined in the switch translations in order for CN-ISVM to work correctly.

11.17 MULTI-LEVEL PRECEDENCE AND PREEMPTION (MLPP) ON SS7

11.17.1 MLPP on SS7 - Stage 1 and Stage 2

The MLPP on SS7 - Stage 1 (99-5E-2844) and MLPP on SS7 - Stage 2 (99-5E-2845) features provide prioritized call handling for SS7 trunks in a 5ESS®-2000 switch. MLPP assigns a priority or precedence level to each call so that it can preempt a call of a lower precedence for one of higher precedence.

Preemption of an SS7 trunk involves the release of a trunk not reserved for reuse (preempt to clear), or the release and reservation for immediate reseizure of a trunk reserved for reuse (preempt for reuse). Preemption may take one of two forms:

- The called party may be busy with a lower precedence call which must be preempted in favor of completing the higher precedence call from the calling party.
- Network resources may be busy with calls, some of which are lower precedence than the call requested by the calling party. One or more of these lower precedence calls may be preempted to complete the higher precedence call.

Both MLPP on SS7 trunk features are available as software updates to the 5E11 and 5E12 software releases. Both features are secured (SFID=196 for Stage 1 and SFID=197 for Stage 2). A right-to-use (RTU) fee must be paid to Lucent Technologies before enabling information is provided.

See 235-190-103, *Business and Residence Feature Descriptions* for a detailed description of the MLPP on SS7 - Stage 1 and Stage 2 features.

Starting in the 5E13 software release, switch personnel have the option to provision the switch to send MLPP Initial Address Messages (IAMs) for calls other than routine with a higher IAM priority than normal traffic.

11.17.2 DSN Centralized Attendant

The DSN Centralized Attendant feature (99-5E-4634) supports a Centralized ISDN Attendant using MLPP SS7 trunks. The feature provides the 5ESS®-2000 switch with the ability to extend ISDN attendant features to include calls that originate from an incoming MLPP SS7 trunk (originator on a different switch from the ISDN attendant):

- The Dial Through Attendant feature (transfer dial tone to originator) allows the ISDN attendant (ISAT) to give a caller access to a private facility and functions only if the customer line is located on the same switch as the ISAT. The DSN Centralized Attendant feature extends the ability of the 5ESS®-2000 switch to use this functionality over MLPP SS7 trunks, allowing a cluster of switches to provide this service using an ISAT physically located at one of the switches in the cluster.
- The Source Billing for Attendant Handled Calls feature substitutes the originator's DN for the attendant's DN in billing records on attendant-transferred calls. The DSN Centralized Attendant feature extends the ability of the 5ESS®-2000 switch to use this functionality over MLPP SS7 trunks by replacing the attendant's billing DN with the remote originator's billing DN in billing records.

Use of the DSN Centralized Attendant feature requires that the Terminal Group Station Restriction for ISUP Trunks feature (SFID = 18) is active so that a terminal group can be used on the incoming MLPP SS7 trunk.

The DSN Centralized Attendant feature is available as a software update to the 5E12 software release. See 235-190-103, *Business and Residence Feature Descriptions* for a detailed description of this feature.

11.18 5ESS®-2000 SWITCH LONG DISTANCE PLATFORM (LDP)

The Long Distance Platform (LDP) feature set (formerly known as toll digital exchange [TDX]) allows a switch to handle basic (POTS) toll calls, along with specialized feature processing on a per customer basis.

The specialized features include:

- per call account codes
- interactions with AIN SCP
- switch-based Network Call Denial
- fixed carrier routing.

The LDP feature set is composed of four subfeatures:

- 99-5E-3127, 5ESS®-2000 Switch Long Distance Platform Basic Call Processing -- is the base feature and is required by the other three features. It contains the basic LDP offering.
- 99-5E-3032, 5ESS®-2000 Switch Long Distance Platform ANI Table Processing -- provides the database for customer specific toll call processing.
- 99-5E-3033, Long Distance Platform ASP Interface -- handles the interface to the SCP.
- 99-5E-3034, Long Distance Platform Account Codes -- allows the LDP switch to collect up to a 15-digit account code from callers and put the code in billing records. This is different from the BRCS Account Code feature. It introduces new interfaces to the RAF Controller code in 5E11.

These are secured features and a right-to-use fee must be paid to Lucent Technologies before enabling information is provided.

There are no changes to CCS7 signaling, but standard CCS7 trunk signaling and TCAP signaling are used to implement this feature. For descriptions of these and other Long Distance Platform features, refer to 235-190-115, *Local & Toll System Features*.

11.19 TCAP MESSAGE TANDEM

11.19.1 Description

The TCAP Message Tandem feature (99-5E-2821) allows a primary 5ESS[®]-2000 Switch Local & Toll System Features switch to send and receive transaction capabilities application part (TCAP) messages to and from a signal transfer point (STP) and route the messages to the appropriate switch in a switch cluster.

This feature allows the STP to process 6-digit global title translations (GTT) when an NPA-NXX is distributed between more than one switch. It minimizes administrative work, especially for small STPs that lack the memory and real-time processing to perform 10-digit GTTs.

This is a secured feature (SFID 195) and a right-to-use (RTU) fee must be paid to Lucent Technologies before enabling information is provided.

11.19.2 Availability

The TCAP Message Tandem feature (99-5E-2821) is available for the 5E11 and later software releases.

11.19.3 Environment

This feature is provided on a per-office basis.

11.19.4 Cross References

The following cross references apply to this feature:

- Feature Number: 99-5E-2821, TCAP Message Tandem

11.19.5 Background

Not applicable.

11.19.6 Feature Operation

The telephone network sends CCS7 message queries, initially routed by directory number (DN), to support local area signaling services (LASS) or interswitch voice messaging (ISVM) subscriber features. The routing of these messages is determined by the CCS7 signal transfer point (STP) from its global title translations (GTT) tables on a number group basis, converting DNs to switch network addresses.

When translating on a number group basis, a single database entry can account for up to 10,000 DNs. When DNs with the same NPA-NXX are shared between different central office switches, the destination DN for these messages cannot be determined based on only the NPA-NXX.

This feature provides an alternate method for routing TCAP messages rather than expanding the STP's GTTs to 10-digit capacity. Even though DNs within a number group are shared between central office switches, all TCAP message queries for a number group are forwarded to a primary 5ESS[®]-2000 switch in a multi-switch cluster for final routing disposition. The 5ESS[®]-2000 switch designated as the TCAP tandem in the cluster analyzes each TCAP message and determines which switch in the cluster serves the DN identified by the message. If the DN belongs to another switch, the TCAP message is reformatted and sent to the serving switch. If the 5ESS[®]-2000 tandem switch serves the DN, the TCAP message is processed normally.

The data needed to perform this routing function is already resident in the switch. Shared DNs that are not resident in the primary switch are translated as route index (RI) entries. This translation will subsequently be referred to as

directory number to route index (DN-RI). The RI information points to the connecting trunk information which contains the point code of the owning switch in the cluster. Thus, the TCAP message is re-routed correctly.

11.19.7 User Operation

11.19.7.1 For Subscribers

No subscriber actions are associated with this feature.

11.19.7.2 For Switch Personnel

The service provider enables this feature using recent change and verify (RC/V).

11.19.8 Engineering

11.19.8.1 Hardware Resources

No hardware considerations are associated with this feature.

11.19.8.2 Software Resources

No software considerations are associated with this feature.

11.19.8.3 Transition Considerations

No transition considerations are associated with this feature.

11.19.9 Interactions and Limitations

The following interactions are associated with this feature:

- (1) For the 5E12 software release, the TCAP Message Tandem feature was enhanced to support NPA splits due to 5E12 differences in NOCCODE definitions. The NXX expansion feature requires the NOCCODE changes that impact the 5E12 software release. During the period when NPA splits are allowed, the old NPA-NXX NOCCODE tuple will exist but the new NPA-NXX tuple will not. The LASS NPA Split Resolution feature (SFID 36) will determine if the new NPA is part of the NPA split.
- (2) The switch performing the TCAP tandem function and redirecting the TCAP message to a new destination will use the point code associated with the ISDN user part (ISUP) trunk based on the first route defined by digit analysis of the called party id. No alternate routing point codes will apply to the TCAP tandeming functions since the ISUP trunk facility is not needed for TCAP message.
- (3) The TCAP tandeming functions are limited to direct ISUP trunks between the tandeming switch and the final destination for the TCAP message.
- (4) The subscriber moved from one switch to another must remain in the same local access and transport area (LATA) in order for the TCAP tandeming functions to operate properly.
- (5) The subsystem number for the application (i.e., LASS) on the TCAP tandeming switch must be identical to the subsystem number for the application on the serving switch (final destination switch for the TCAP message).
- (6) To avoid TCAP looping situations due to provisioning errors, it is recommended that the TCAP Tandem feature be used to migrate lines from one switch to one switch. In addition, this feature should be active on only one of the switches in a pair of switches where lines are being migrated from one switch to the other.

- (7) For full LASS/ISVM compatibility, the destination switch must support the capabilities described in "Dependencies," Section 11.19.11 .

11.19.10 Incompatibilities

No incompatibilities are associated with this feature.

11.19.11 Dependencies

For full LASS/ISVM compatibility, the destination switch must be able to:

- (1) Define a directory number or line (or similar mechanism such as hundreds route index) to route via a CCS7 trunk group to the 5ESS[®]-2000 switch with TCAP Tandem functionality.
- (2) When a line at the destination switch dials the LASS automatic recall (AR) access code, the switch sends a LASS TCAP message when the AR number is a DN-RI.

When a line at the destination switch dials the LASS automatic callback (AC) access code, the switch sends a LASS TCAP message when the AC number is a DN-RI.

When a line at the destination switch adds a number to a LASS screening list that would route via a DN-RI, the switch sends a LASS TCAP message.

If the switch denies any of these criteria, some LASS functionality will be lost.

- (3) When the destination switch has the interswitch voice message (ISVM) capability and a voice message system (VMS) attempts to activate or deactivate a number translated as a DN-RI, the switch sends a ISVM TCAP message.

If the switch denies this criterion, some ISVM functionality will be lost.

The Lucent 1A ESSTM destination switch meets criteria 1 through 3 when the office option's TQSNXX (TCAP Query Shared NXX) bit is set.

A 5ESS[®]-2000 destination switch without TCAP Tandem using DN-RIs does not meet criteria 1 through 3. However, the use of hundreds route indexes (RC view 4.14) will meet these criteria.

For non-Lucent destination switches, the switch owner and vendor need to determine the compatibility with criteria 1 through 3. If any of these criteria are denied at the destination switch, full LASS or ISVM compatibility will not be preserved with TCAP Tandem.

11.19.12 Isolation Constraints

No isolation constraints are associated with this feature.

11.19.13 Recent Change Provisioning

11.19.13.1 TCAP Tandem Provisioning

See 235-118-2xx, *Recent Change Reference* , for detailed information on allowed values.

The service provider enables the TCAP Message Tandem feature by populating the following fields in RC/V view 8.22 (SECURED FEATURE UPGRADE):

FIELD	VALUES
FEATURE ID	195
MODULE	OFC
PASSWD	(Obtain from Lucent Technologies SFID Administrator)
ACTIVE	Y

11.19.13.2 Destination Switch Provisioning

11.19.13.2.1 General

The destination switch can be any vendor switch. However, its compatibility with LASS and ISVM must be determined as described in "Dependencies," Section 11.19.11 .

For lines that have been re-located to a 5ESS®-2000 switch with switch TCAP Tandem functionality, the destination switch will use a DN-RI or similar mechanism (for example, hundreds route index) to access a CCS7 trunk group to the TCAP Tandem switch. Lines with office equipment will complete locally (as they did prior to TCAP Tandem).

11.19.13.2.2 Lucent 1A ESS™ Switch as a Destination Switch

A Lucent 1A ESS™ switch is LASS/ISVM compatible when the office option table's TQSNXX (TCAP Query Shared NXX) bit is set. This permits TCAP messages to be sent when DN-RIs are encountered.

11.19.13.2.3 Lucent 5ESS®-2000 Switch as a Destination Switch

A Lucent 5ESS®-2000 destination switch without TCAP Tandem has DN-RIs but will not send the TCAP messages needed for full LASS/ISVM compatibility. Hundred RTIs (RC view 4.14 - HRI) can be used and will generate the TCAP messages necessary for LASS/ISVM compatibility.

HRIs will cause all unallocated numbers within the hundreds group to route to the 5ESS®-2000 switch with TCAP Tandem for intercept treatment. When using HRIs, care must be taken to prevent trunk looping situations. For example, a destination switch and TCAP Tandem switch using HRIs for the same hundreds group would have a trunk looping condition for unallocated numbers.

11.19.14 Customer Premises Equipment (CPE)

Not applicable.

11.19.15 Maintenance Considerations

Not applicable.

11.19.16 Administration

11.19.16.1 Measurements

This feature does not impact measurements.

11.19.16.2 Billing

This feature does not impact billing.

11.20 CALL INFORMATION DISPLAY FEATURE

11.20.1 Description

The Call Information Display (CID) feature (99-5E-4382) collects real-time call data for actual test calls. CID collects call processing data including digit analysis data, TCAP data, ISUP data, and selected routing data. After the data is collected, a switch-resident formatting script translates the data into a readable format and prints it on the ROP. The CID feature uses existing 5ESS®-2000 switch OSDS monitor commands for feature overhead such as setup, SM data buffering, and SM-to-AM data transport.

CID is a secured feature (SFID 208) and a right-to-use (RTU) fee must be paid to Lucent Technologies before enabling information is provided.

11.20.2 Availability

The Call Information Display feature (99-5E-4382) is available for 5E11 and later software releases.

11.20.3 Environment

This feature is provided on a per-office basis.

11.20.4 Cross References

The following cross references apply to this feature:

- Feature Number: 99-5E-4382

11.20.5 Background

Not applicable.

11.20.6 Feature Operation

CID collects call data in the SM specified during feature setup. For originating data collection such as line and trunk originations, CID is set up in the SM that the line resides in, or in the SM/SMs that contain the incoming trunk group. For terminating data collection such as line and trunk terminations, CID is set up in the SM that the terminating line resides in, or in the SM/SMs that contain the outgoing trunk group.

NOTE: When CID is set up for originating data collection such as on an originating line or incoming trunk group, the terminating data for a given test call is collected automatically. For example, for a test call that originates on a line in SM 1 and leaves the switch on an outgoing trunk in SM 5, CID prints setup messages and collects data in SM 1 and SM 5.

CID can isolate a single test call in one of three ways:

- by specifying the originating or terminating port of the related line or trunk
- for ISUP trunk originations and terminations, by specifying the calling or called number of the test call
- for line or MF trunk originations, by specifying the called number of the test call.

When CID is set up and a test call is made, a setup message is displayed on the ROP to notify the user that the feature has been activated on a specific port in a specific SM:

```
REPT: CALL INFORMATION DISPLAY SETUP
PORT=H'XXX, SM=Y
```

where XXX is the port number (in hexadecimal) and Y is the SM number.

This message indicates that the CID feature is active and that the requested data will be collected in the SM specified by the output message.

11.20.7 User Operation

11.20.7.1 For Subscribers

No subscriber actions are associated with this feature.

11.20.7.2 For Switch Personnel

To collect test call data with the Call Information Display feature:

- (1) Set up a test line to simulate the type of call for which data collection is needed. Obtain the related port address for that line, or, for trunk-based data collection, the related port address of the trunk. For calling/called number filters, no port address is needed.
- (2) Determine the filter mechanism:
 - For port filtering, CID isolates the test call by the SM and port number entered during feature setup. In a given SM, when CID recognizes that the current call is related to the test line/trunks port, data collection is activated.
 - For calling/called number filtering, CID checks the calling or called number against the number entered during feature setup. If the numbers match, data collection is activated.

NOTE: For most call scenarios, filter mechanisms only need to be set up on the originating side of the call (in other words, on the originating line or incoming trunk). CID automatically activates data collection in the terminating line's SM (TAT data collection) or the outgoing trunk's SM. A separate CID setup message indicates that data collection is activated in the SM of the terminating line or the outgoing trunk.

- (3) Determine the method of data collection. By default, CID appends the data stored in the SM for each test call. To reset the data collection buffer, set the dmh flag in the monitor setup command line. Example:

```
set:mon,sm=xxx,wtd,dap,dmh,ctl=on;
```

- (4) Allow the trace with the following command lines.

— For port filtering:

```
clr:mon:sm=xxx,all;
set:mon,sm=xxx,wtd,dap,ctl=on;
set:mon,sm=xxx,data,prt=h'pppp;
alw:mon,sm=xxx;
```

— For ISUP filtering on the calling number:

```
clr:mon:sm=xxx,all;
set:mon,sm=xxx,wtd,dap,ctl=on;
```

```
set:mon,sm=xxx,spec,s00=A,s01=B;  
alw:mon,sm=xxx;
```

— For filtering on the called number (lines or MF/ISUP trunks):

```
clr:mon:sm=xxx,all;  
set:mon,sm=xxx,wtd,dap,ctl=on;  
set:mon,sm=xxx,spec,s03=C,s04=D;  
alw:mon,sm=xxx;
```

— For filtering on a variable length called number (such as an international number):

```
clr:mon,sm=xxx,all;  
set:mon,sm=xxx,wtd,dap,ctl=on;  
set:mon,sm=xxx,spec,s02=E,s03=F,s04=G;  
alw:mon,sm=xxx;
```

where:

pppp

- for line or trunk originations — is the originating line or incoming trunk port number
- for line and trunk terminations — is the terminating line or outgoing trunk port number
- for ISDN line terminations to lines with ASP Termination Attempt Triggers assigned — is the D-channel port number
- for ISDN originations — is the B1-channel port number

A is the *calling* number NPA from which the test call is being made. For ISUP data collection on CCS7 trunk calls only.

B is the 7-digit *calling* number from which the test call is being made (if A and B are entered, the prt parameter is not needed). For ISUP data collection on CCS7 trunk calls only.

C is the *called* number NPA to which the test call is being made.

D is the 7-digit *called* number to which the test call is being made (if C and D are entered, the prt parameter is not needed).

E is the number of digits (range: 7 through 15) entered for the called number filter.

F is digits 1 through 8 of the called number.

G is digits 9 and higher (up to 15) of the called number (if called number is greater than 8 digits in length).

- (5) Make a test call. After the test call is made, execute the following command to transport data from the SM (where it is collected) to the AM (where the formatting script translates the data into a readable format):

```
op:mon,sm=xxx,dsp,dpf=1000,fn="/usr/tmp/smmon";
```

NOTE: To download the maximum data buffer size (for extensive TCAP/ISUP scenarios), replace

dpf=1000 with the dpa parameter.

NOTE: If CID data is collected in multiple SMs, execute the download and format commands for the originating SM, then the terminating SM, or specify a separate file name for each SM's data.

NOTE: File `/usr/tmp/smmon` is the default AM file to which all SM data is downloaded. Users have the option to put the data in a different AM directory and file, but the full path name must be specified and it is the user's responsibility to ensure that write and read permissions are set for the directory used.

- (6) After the `OP:MON:DSP... COMPLETE` message prints on the ROP, enter the following command to print the formatted data on the ROP:

```
exc:envir,uproc,fn="/no5text/cni/proc/CIDFMT",opl=20;
```

NOTE: The above command assumes that the default AM file was used in the previous `op:mon:sm...` `fn="/usr/tmp/smmon";` command. If the user downloads the SM data to a different file, then the appropriate path and file name must be specified as an argument:

```
exc:envir:uproc,fn="/no5text/cni/proc/CIDFMT",opl=20,
ARGS="[full_path/]file_name";
```

If the full path name is not specified, the formatting tool expects the file to be in the `/usr/tmp` directory on the AM.

NOTE: For TCAP data collection, users have the option to print the SCCP header information. The default output does not print because of ambiguous SCCP header data on *outgoing* TCAP messages (incoming TCAP messages have valid SCCP header data). To print the SCCP header information, the `-a` argument must be specified:

```
exc:envir:uproc,fn="/no5text/cni/proc/CIDFMT",opl=20,
ARGS="-a-[full_path/]file_name";
```

- (7) For subsequent test calls, repeat steps 5 and 6.

11.20.7.2.1 EXAMPLES

- (1) Collect CID data on a test call originating from port h'14d:

```
clr:mon:sm=xxx,all;
set:mon,sm=xxx,wtd,dap,ctl=on;
set:mon,sm=xxx,data,prt=h'14d;
alw:mon,sm=xxx;
```

- (2) Collect CID data on a test call originating from the number 630-555-2264:

```
clr:mon:sm=xxx,all;
set:mon,sm=xxx,wtd,dap,ctl=on;
set:mon,sm=xxx,spec,s00=630,s01=5552264;
alw:mon,sm=xxx;
```

- (3) Collect CID data on a test call to the 14-digit international number 011-31-20-123-4567:

```
clr:mon,sm=xxx,all;
set:mon,sm=xxx,wtd,dap,ctl=on;
```

```
set:mon,sm=xxx,spec,s02=14,s03=01131201,s04=234567;  
alw:mon,sm=xxx;
```

11.20.8 Engineering

11.20.8.1 Hardware Resources

No hardware considerations are associated with this feature.

11.20.8.2 Software Resources

No software considerations are associated with this feature.

11.20.8.3 Transition Considerations

No transition considerations are associated with this feature.

11.20.9 Interactions and Limitations

No interactions or limitations are associated with this feature.

11.20.10 Incompatibilities

No incompatibilities are associated with this feature.

11.20.11 Dependencies

No other features need to be installed or activated in order for this feature to work.

11.20.12 Isolation Constraints

No isolation constraints are associated with this feature.

11.20.13 Recent Change Provisioning

The service provider enables the Call Information Display feature by populating the following fields in RC/V view 8.22, SECURED FEATURE UPGRADE:

FIELD	VALUES
FEATURE ID	208
MODULE	OFC
PASSWD	(Obtain from Lucent Technologies SFID Administrator)
ACTIVE	Y

11.20.14 Customer Premises Equipment (CPE)

Not applicable.

11.20.15 Maintenance Considerations

Not applicable.

11.20.16 Administration

11.20.16.1 Measurements

This feature does not impact measurements.

11.20.16.2 Billing

This feature does not impact billing.

12. SS7 ACCESS ON A PACKET SWITCH UNIT (PSU) PLATFORM

FEATURE DESCRIPTION

SS7 access on a PSU platform introduces switching module (SM)-based SS7 signaling, where signaling links terminate on a resident packet switch unit (PSU) platform.

SM-based SS7 signaling is available in both the 5ESS[®]-2000 switch Very Compact Digital Exchange (VCDX) and 5ESS[®]-2000 switch environments as implemented by these features:

- SS7-PSU in a VCDX Environment, feature number 99-CP-2345
- SS7-PSU on SM/EXM-2000, feature number 99-5E-3114
- Call/Circuit Monitor, feature number 99-5E-3114.B (see Section 8.2)
- SS7-PSU Maintenance and Reliability Enhancements, feature number 99-CP-4246.B
- SS7-PSU MTP and SCCP Routing Verification Tests, feature number 99-CP-4246.E
- PH22 Base, feature number 97-5E-4286
- PH22 SCCS Software Image Support, feature number 99-5E-4302
- SS7-PSU Link Enhancements, feature number 97-CP-4246.K
- SS7-PSU Whitebook MTP Enhancements, feature number 99-5E-4238
- PSU2 Direct Software Update, feature number 97-CP-4463.

For information on PSU-based SS7 in the Distinctive Remote Module (DRM), refer to the 5ESS[®]-2000 Switch Distinctive Remote Module User's Guide, 235-200-150.

SS7-PSU in a VCDX Environment, 99-CP-2345 (available in the 5E11 and later software releases) converts an "ordinary" 5ESS[®]-2000 switch Very Compact Digital Exchange (VCDX) office into a VCDX with CCS7 access on a PSU. Prior to this feature, the SM of a VCDX switch could not support common channel signaling (CCS) functions.

The VCDX feature adds a broad range of CCS functions, using existing packet switching and peripheral access hardware on the VCDX SM/SM-2000. This feature adds these CCS functions:

- ISDN user part (ISUP) and transaction capabilities application part (TCAP) services.
- A hardware/software platform, resident on the VCDX SM/SM-2000, to support the first three layers of the message transfer part (MTP) protocol, and the connectionless procedures for signaling connection control part (SCCP) services, required by SS7 end offices.
- The ability to provision/maintain signaling routes and trunk routes in a VCDX environment. CCS signaling links (CCSLKs) use digital facility interface (DFI) or SM-2000 digital networking unit - SONET (DNU-S) facilities on the SM-2000 as access, and are terminated on a packet switch unit (PSU).

SS7-PSU on SM/EXM-2000, 99-5E-3114 (available in the 5E12 and later software releases) extends SM-based SS7 signaling described above to any SM/SM-2000 in a 5ESS[®]-2000 switch. This feature adds this functionality:

- Any 5ESS[®]-2000 switch SM/SM-2000 can be provisioned with an SM-based signaling interface. This includes a

hardware and software platform identical to that introduced in the 5ESS®-2000 switch VCDX implementation. Such an SM possesses its own unique originating point code (OPC), and controls selected ISUP trunk groups terminated on that SM. Such trunks can be globally or locally hunted, and can coexist with trunks controlled by the CNI on the same SM.

In the unlikely event that a switching module loses connectivity to the communication module (CM) or the administrative module (AM), any trunks controlled by the CNI would be nonfunctional. However, those trunks supported by the PSU platform SS7 interface would continue to support call processing in stand-alone mode.

- The feature also provides TCAP enhancements, support of AT&T point code formats, and new MTP/SCCP measurements. These enhancements (described in detail in other sections) are available to VCDX offices, as well as 5ESS®-2000 switching modules, beginning in the 5E12 software release.

Call/Circuit Monitor, 99-5E-3114.B (available in the 5E12 and later software releases) provides protocol monitoring options and capabilities for the monitoring and maintenance of SS7 signaling based network services. It applies to PSU SS7 and adds to capabilities available for Common Network Interface (CNI). Service providers can perform traps on SS7 calls for the duration of the call, analyze SS7 problems, and receive monitoring results in English text rather than the hexadecimal format previously used (see Section 8.2).

With this feature, the customer has the ability to monitor inbound and outbound Transaction Capabilities Application Part (TCAP) queries based on called/calling party information found in either the SCCP header or TCAP data part of the TCAP query message.

Because calling party information is optional in the SCCP header (the 5ESS®-2000 switch implementation does not provide it) but required in the TCAP data part of the query, the customer will have the ability to specify a specific called/calling party to be found in the TCAP data part and then begin protocol monitoring. For example, the customer can monitor a specific subscriber calling an 800 number rather than having to monitor all subscribers calling the 800 number to find information on one specific subscriber.

The TCAP data part is limited to TCAP queries originated by the switch and thus outbound to the SS7 network. The capability to monitor inbound TCAP queries based on called/calling party information in the TCAP data part is not provided.

In addition, the customer has the ability to monitor inbound and outbound ISDN User Part (ISUP) messages relating to a particular call based on called/calling party information.

SS7-PSU Maintenance and Reliability Enhancements, 99-CP-4246.B (available in 5E13 and later software releases) provides some maintenance enhancements for the existing PSU signaling platform. This feature adds this functionality:

- Elimination of false signaling link congestion.
- Improved signaling link test procedures.
- Improved signaling link failure reports.
- New conventions for describing digital networking unit — SONET (DNU-S) components.

SS7-PSU MTP and SCCP Routing Verification Tests, 99-CP-4246.E (available in 5E13 and later software releases) activates the Operational, Maintenance and Administration Part (OMAP) functionality for existing PSU signaling platforms. This feature adds this functionality:

- The availability of the MTP Routing Verification Test, which checks the accuracy/consistency of the administrable message transfer part (MTP) routing data to far-end signaling points.

- The availability of the SCCP Routing Verification Test, which provides a mechanism to test signaling connection control part (SCCP) routing data for accuracy, consistency, and completeness in handling local global title translation requests.

PH22 Base, 97-5E-4286 and PH22 SCCS Software Image Support, 99-5E-4302 (available in 5E14 and later software releases) provide the PH version 22 (PH22) protocol handler hardware, which can be used to support CCS channel groups. The PH22 has enhanced latency/throughput characteristics and more memory than PH3 hardware. The PH22 is required to support SS7-PSU MTP Capacity and Routing Enhancements (feature 97-CP-4246.K) introduced in the 5E14 software release.

SS7-PSU Link Enhancements, 97-CP-4246.K (available in 5E14 and later software releases) provides capacity and routing enhancements for SS7 PSU signaling platform to achieve feature parity with capabilities offered on the CNI signaling platform. This feature adds this functionality:

- Signaling Link Selector (SLS) Code Expansion — Allows the SS7 PSU load sharing procedures to support the 8 bit SLS code field and load share the traffic evenly across the available links.
- Increase Linkset Size to 16 Links — Allows the SS7 PSU signaling platform to support up to 16 links per linkset.
- Label A/E/F Links — Allows the labeling of links according to their link type.
- ISUP Message Handling in the PSU — Allows MTP to respond with ISUP Release (REL) messages to fail incoming call set-up requests when it determines it cannot route the message to the appropriate SM.

SS7-PSU Whitebook MTP Enhancements, 99-5E-4238 (available in 5E14 and later software releases) ports the Whitebook MTP enhancements provided by international features i1312-128, i1312-123, i1312-124, and i1131-157 to the North American Region (NAR) market. This feature provides Message Transfer Part (MTP) Node Restart procedure, Short Term Processor Outage procedure, MTP User Part Unavailable (UPU) procedure, and Signaling Connection Control Part (SCCP) Remote Subsystem Number (SSN) Status procedure. Refer to Section 12.4 for provisioning information.

- The MTP Node Restart procedure provides protection for the node whose MTP is restarting, and for the network by giving the restarting node time to activate sufficient signaling links and to exchange enough routing data with the network before user traffic is restarted to avoid message loss and mis-sequencing. Two signaling network management messages, TRW (Traffic Restart Waiting) and TRA (Traffic Restart Allowed), are used in conjunction with MTP Level 3 timers T25, T28, and T29 and other network management messages to control the procedure. The 5ESS[®]-2000 switch for the North American Region (NAR) supports only the Adjacent MTP Node Restart (ANSI[®]) procedure at this time. Controls are provided to allow or disable the feature. This is a secured feature (SFID=177).
- The Short Term Processor Outage procedure reduces the amount of time required to recover from a processor outage state. When a processor outage occurs, the MTP Level 3 timer T1 (500-1200 ms) is used to determine the severity of the outage. If the outage clears prior to T1 expiration, the outage is considered to be sufficiently short enough that service may be immediately resumed, no changeover occurs, and any in-progress changeovers are aborted. Also, no MTP Node Restart procedure is initiated. Messages in the transmit and re-transmit buffers are preserved and transmitted when the outage clears. However, if timer T1 does expire, new traffic should be delivered to an alternate route. When the outage does clear, any buffered messages associated with the failed link are considered to be too old to be useful and must be discarded. Controls are provided to allow or disable the feature, which is defaulted as "allowed."
- The MTP User Part Unavailable procedure provides for when the MTP is unable to distribute a received message to a local user because that user is unavailable, (for example: no ISUP trunks defined, SCCP is

currently unavailable). The MTP sends a User Part Unavailable (UPU) message to the MTP at the originating signaling point. The detailed information regarding whether the user is unequipped or unavailable for management reasons is contained in the UPU message. No controls are provided to allow or disable the feature.

- The SCCP Remote SSN Status procedure is dependent on the MTP User Part Unavailable procedure. This procedure provides for management of remote SCCP statuses (the status of the SCCP "process" at a remote signaling point). When a message is sent to a signaling point whose SCCP is unavailable, the MTP at that signaling point returns a UPU message. When that message is received by the local MTP, it provides an MTP-STATUS indication to the local SCCP with an indication of the unavailable user (the remote SCCP). When an MTP-STATUS is received indicating that the remote SCCP is unavailable, all subsystems at that signaling point must be marked as prohibited (as is done when the signaling point itself becomes unavailable). In addition, the status of the remote SCCP is also marked as prohibited. A Subsystem Status Test (SST) must then be initiated for the concerned SSN=1 (Sub System Number), and all SSTs for other prohibited subsystems at that signaling point must be stopped. If the remote SCCP is still unavailable, a UPU is returned. If an SST for SSN=1 is received, then an SSA (Sub System Allowed) for SSN=1 is returned and existing procedures for the handling of subsystems after a signaling point recovery should be followed. If an SSA (SSN=1) is received, then the remote SCCP is marked as allowed and all subsystems at that signaling point are also marked as allowed. Controls are provided to allow or disable the feature.

PSU2 Direct Software Update, 97-CP-4463 (available in 5E14 and later software releases) improves SS7 reliability by allowing a software update (SU) pump to occur without loss of signaling capability.

When a software update was executed on the switch in previous software releases, the protocol handler (PH) was taken out of service to download the new image. The PSU2 Direct Software Update feature allows the PH to remain in service to process SS7-based calls during the software update. This feature improves service for customers on the VCDX platform and those with EXM PSU signaling.

This feature builds upon the SS7 on PSU (99-CP-2345) feature for the 5ESS[®]-2000 switch Very Compact Digital Exchange (VCDX) in the 5E11 software release and the SS7-PSU for SM/EXM-2000 (99-5E-3114) feature in the 5E12 software release. The capability is functional for PSU2-based PHs only.

CROSS REFERENCES

These features provide SS7 signaling access on a PSU platform:

- 99-CP-2345, SS7-PSU in a VCDX Environment
- 99-5E-3114, SS7-PSU on SM/EXM-2000
- 99-5E-3114.B, Call/Circuit Monitor
- 99-CP-4246.B, SS7-PSU Maintenance and Reliability Enhancements
- 99-CP-4246.E, SS7-PSU MTP and SCCP Routing Verification Tests
- 97-5E-4286, PH22 Base
- 99-5E-4302, PH22 SCCS Software Image Support
- 97-CP-4246.K, SS7-PSU Link Enhancements
- 99-5E-4238, SS7-PSU Whitebook MTP Enhancements
- 97-CP-4463, PSU2 Direct Software Update

BACKGROUND

Not applicable.

AVAILABILITY

The features that provide SS7 access on a PSU platform are:

- SS7-PSU in a VCDX Environment, 5E11 and later software releases
- SS7-PSU on SM/EXM-2000, 5E12 and later software releases
- Call/Circuit Monitor, 5E12 and later software releases (this is a secured feature that must be purchased before it can be activated)
- SS7-PSU Maintenance and Reliability Enhancements, 5E13 and later software releases
- SS7-PSU MTP and SCCP Routing Verification Tests, 5E13 and later software releases
- PH22 Base, 5E14 and later software releases
- PH22 SCCS Software Image Support, 5E14 and later software releases
- SS7-PSU Link Enhancements, 5E14 and later software releases
- SS7-PSU Whitebook MTP Enhancements, 5E14 and later software releases
- PSU2 Direct Software Update, 5E14 and later software releases.

FEATURE ENVIRONMENT

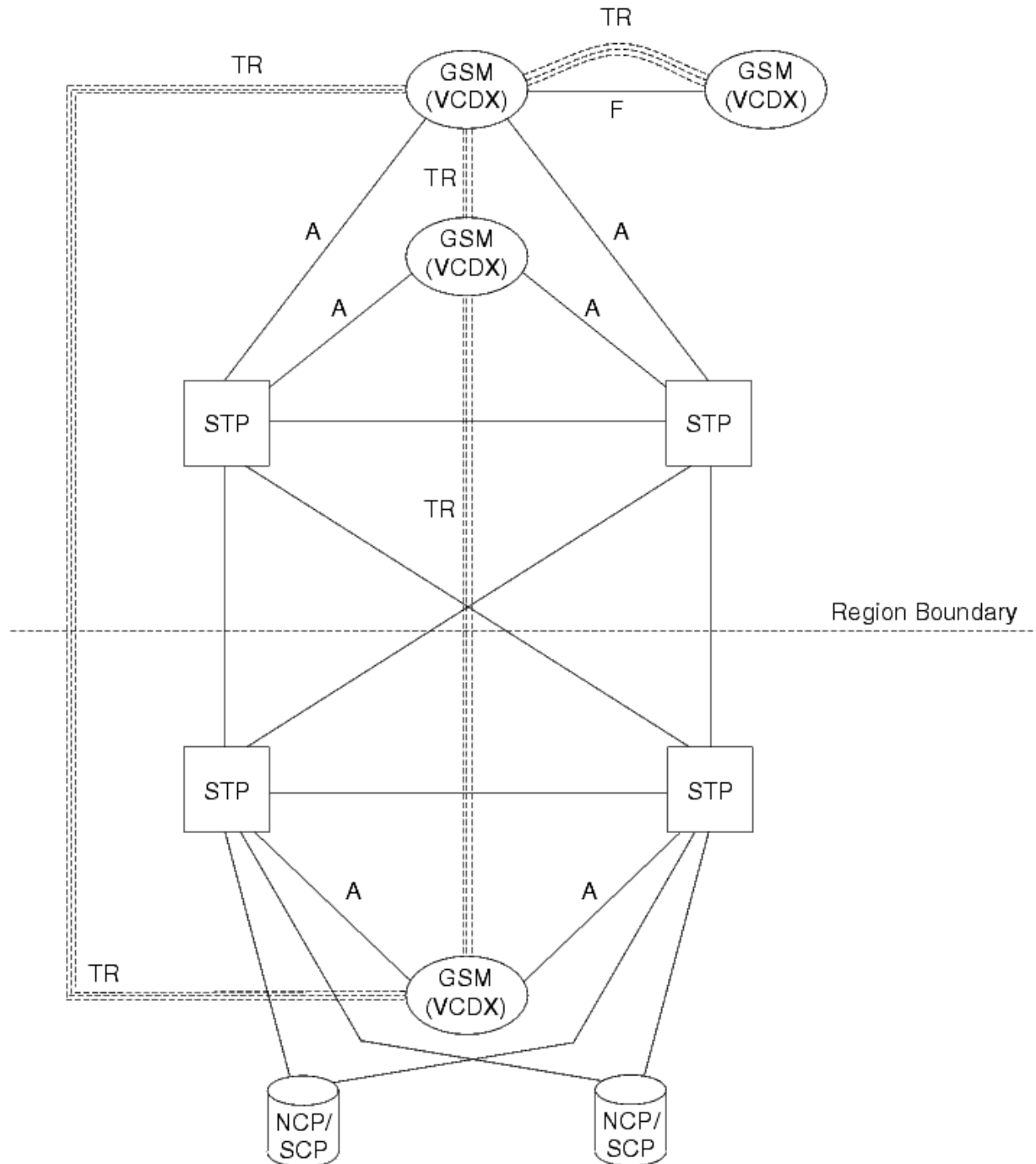
SS7 on PSU is provided per office in the 5ESS[®]-2000 switch Very Compact Digital Exchange (VCDX) environment in 5E11 and later software releases, and per SM/SM-2000 on the 5ESS[®]-2000 switch in 5E12 and later software releases.

12.1 FEATURE OPERATION

12.1.1 General Description of CCS7 Network Operation

The purpose of a CCS network is to transmit all of the signaling information for a group of trunks over a channel that is completely separated from the voice/data communication path. The CCS network also transmits detailed logic and data used to provide diversified calling features/services (such as 800 call routing). See "Signaling System 7 (SS7) Overview," Section 2, of this document for a detailed description of general CCS network attributes.

The information that follows highlights the use of a global switching module (GSM) in the CCS network. A GSM indicates a PSU platform for SS7 signaling is provisioned. In the 5E11 software release, a GSM can be provisioned only on a 5ESS®-2000 switch Very Compact Digital Exchange (VCDX), while any 5ESS®-2000 switching module may be equipped as a GSM in the 5E12 software release.



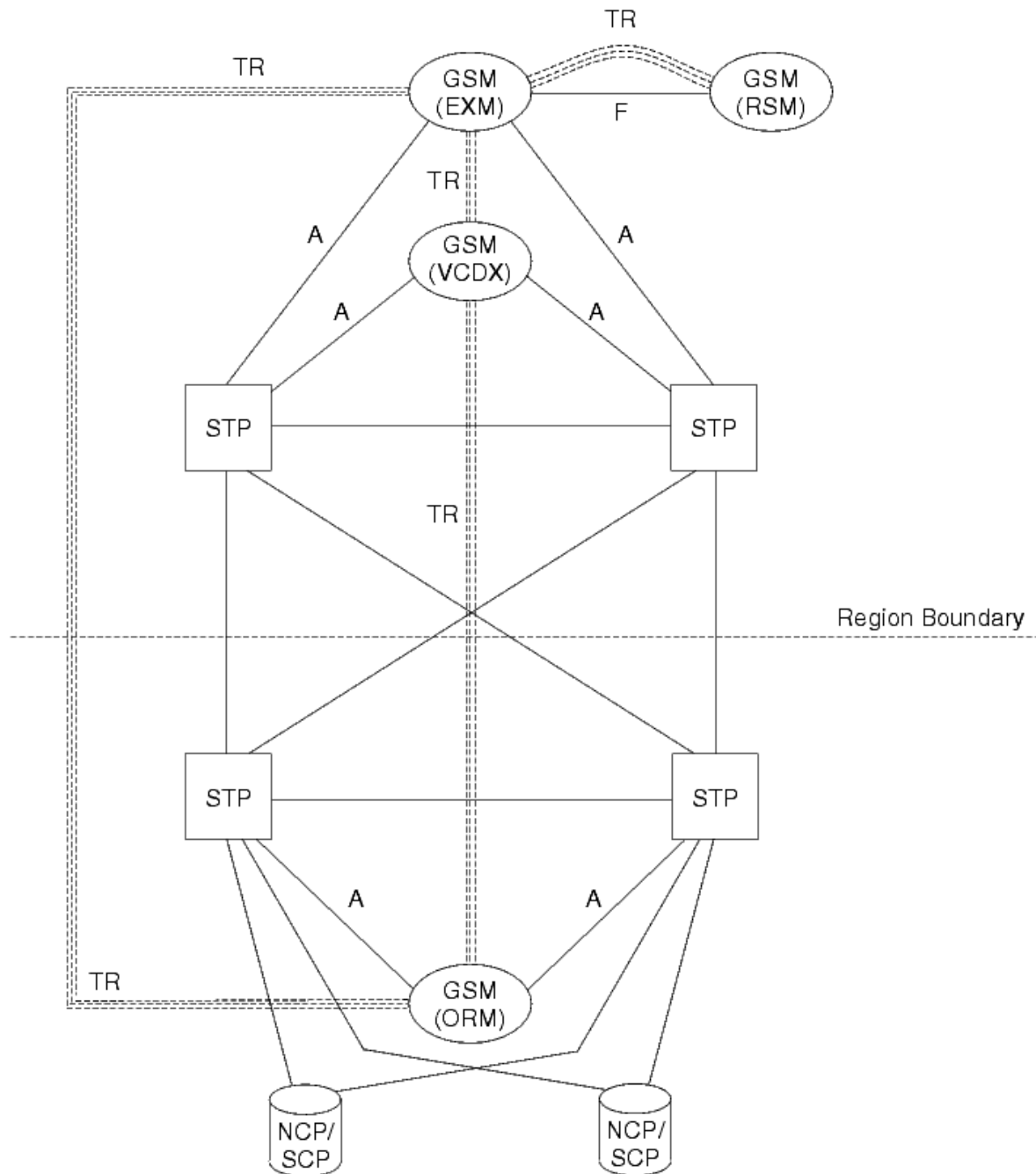
Legend

A - Access Signaling Links
 F - Direct Signaling Links
 GSM - Global Switching Module
 NCP/SCP - Network Control Point/Service Control Point
 STP - Signal Transfer Point
 TR - ISUP Trunk Routes
 VCDX - Very Compact Digital Exchange with CCS Access on a PSU Platform

Figure 12.1-1 Typical VCDX CCS Network Configuration 5E11 Software Release 5E11 VCDX CCS network

configuration

Figure 12.1-1 illustrates the placement of a VCDX office in a regional CCS network in the 5E11 software release, while Figure 12.1-2 illustrates general GSMs possible in the 5E12 software release.



Legend

A - Access Signaling Links
 EXM - Extended Switching Module - 2000
 F - Direct Signaling Links
 GSM - Global Switching Module
 NCP/SCP - Network Control Point/Service Control Point
 ORM - Optically-Integrated Remote Switching Module
 RSM - Remote Switching Module
 STP - Signal Transfer Point
 TR - ISUP Trunk Routes
 VCDX - Very Compact Digital Exchange

Figure 12.1-2 Typical GSM CCS Network Configuration 5E12 Software Release 5E12 GSM CCS network configuration

Although other SS7 office equipment can also be used to link signaling points only GSMs are shown in these figures. These characteristics should be noted:

- The GSM possesses a unique **point code**, to identify it as a signaling termination in the CCS network.
- The GSM can only play the role of a signaling end point (SEP). It provides a signaling link termination that sends/receives signaling messages to configure voice/data trunks necessary to complete a call. It can also request or receive the logic or data necessary to provide special services (such as 800 call routing).

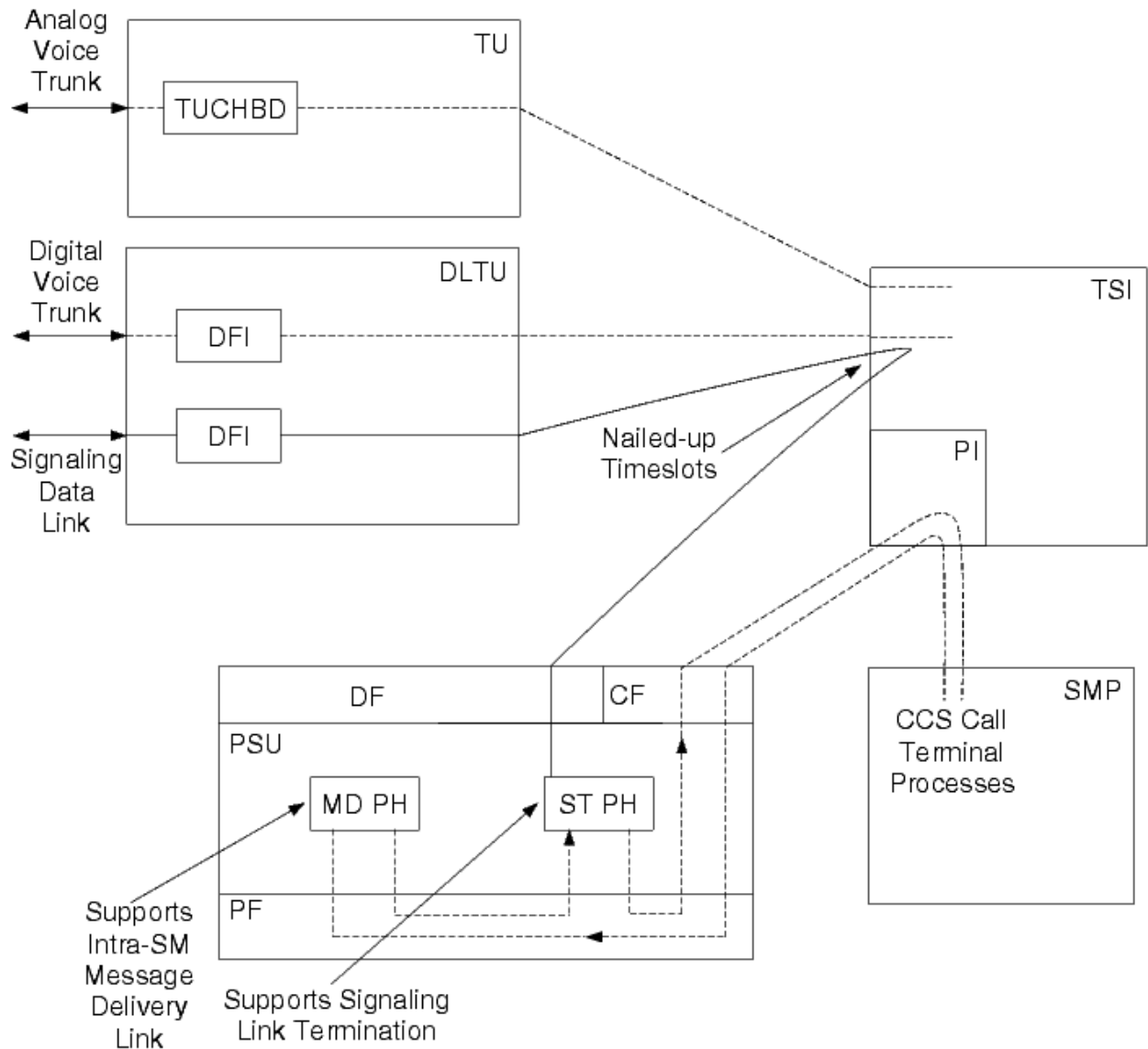
All signaling messages arriving at a GSM must have the GSM's point code as a destination. The GSM **cannot** contain the data or logic necessary to complete TCAP queries from other offices, nor does it have direct connections to sites possessing that data.

- A GSM can provide **associated signaling** to another office, which implies the signaling path and the voice/data trunks terminate in the same far-end exchange, by provisioning direct signaling links (F-Links).
- A GSM can use **quasi-associated signaling** as its primary signaling vehicle. This method allows signaling paths to terminate on an exchange/STP, which is an office that does not terminate voice/data trunks. The choice of the signaling route is predetermined, and it is assumed the far-end is able to transfer messages toward the ultimate destination.

Typical access is to STPs through access signaling links (A-Links); these STPs, in turn, provide direct/indirect access to other switching offices (including other GSMs), or to network control point (NCP)/service control point (SCP) data bases necessary for special services.

12.1.2 PSU Hardware Platform

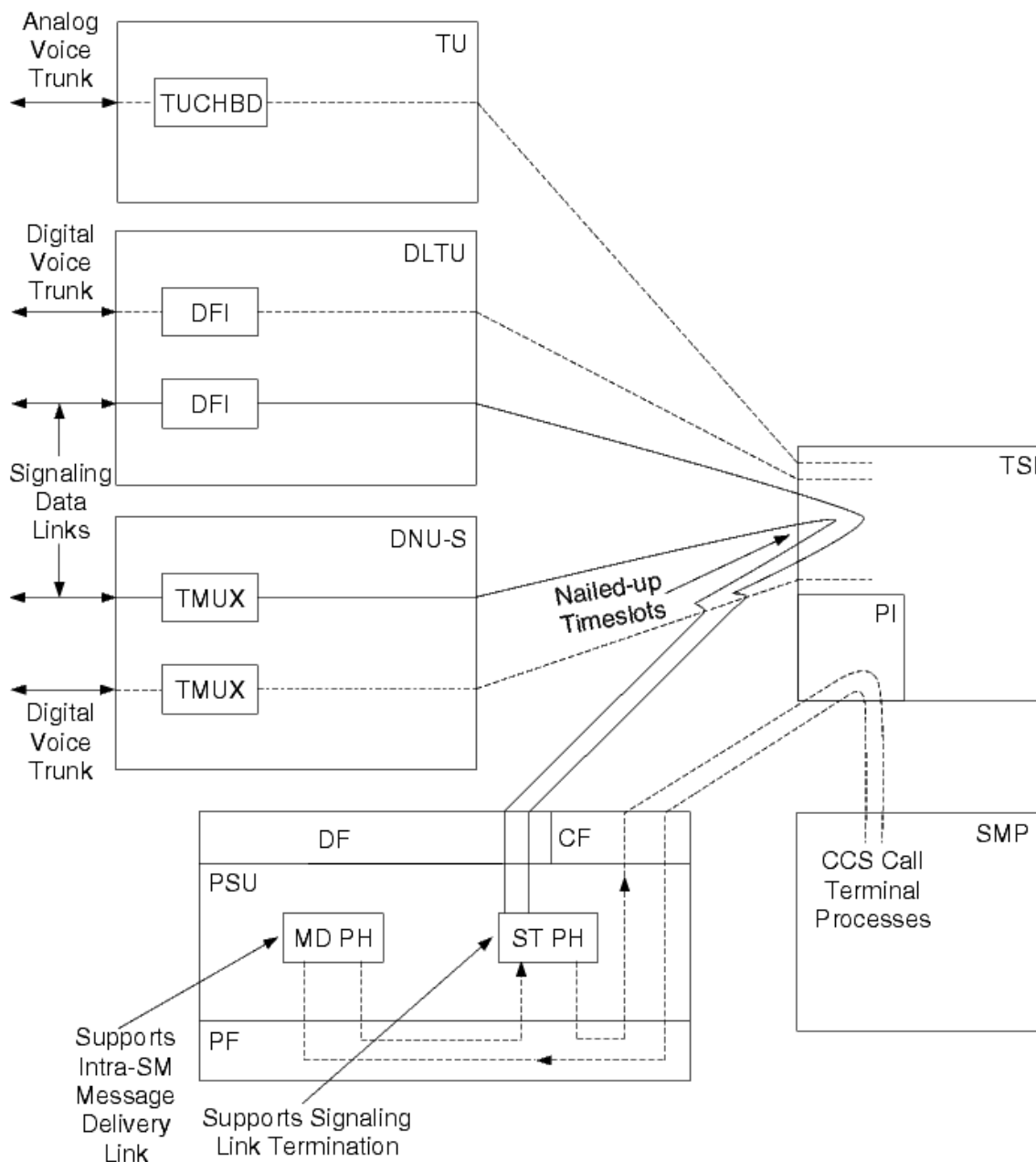
The component hardware necessary to support CCS signaling links (CCSLKs) in a GSM is described in this section. Figure 12.1-3 illustrates the interconnection of components in an SM and Figure 12.1-4 shows interconnection in an SM-2000.



Legend

CF - Control Fanout	PSU - Packet Switch Unit
DF - Data Fanout	SM - Switching Module
DFI - Digital Facility Interface	SMP - Switching Module Processor
DLTU - Digital Line Trunk Unit	ST PH - Signaling Terminal Protocol Handler
MD PH - Message Delivery Protocol Handler	TSI - Timeslot Interchange Unit
PF - Packet Fanout	TU - Trunk Unit
PI - Packet Interface	TUCHBD - TU Channel Board

Figure 12.1-3 GSM Signaling Link Architecture (SM) GSM signaling link architecture (SM)



Legend

CF - Control Fanout
 DF - Data Fanout
 DFI - Digital Facility Interface
 DLTU - Digital Line Trunk Unit
 DNU-S - Digital Networking Unit-SONET
 MD PH - Message Delivery Protocol Handler
 PF - Packet Fanout
 PI - Packet Interface

PSU - Packet Interface Unit
 SM - Switching Module
 SMP - Switching Module Processor
 ST PH - Signaling Terminal Protocol Handler
 TMUX - Transmission Multiplexer
 TSI - Timeslot Interchange Unit
 TU - Trunk Unit
 TUCHBD - TU Channel Board

Figure 12.1-4 GSM Signaling Link Architecture (SM-2000) GSM signaling link architecture (SM-2000)

The components shown include:

- GSM access to/from the external signaling network is through 56 Kbps or 64 Kbps (kilobits per second) digital channels, called signaling data links (SDLs).

These SDLs may enter an SM or SM-2000 as a DS0 channel on a T1 trunk terminated on a resident digital facility interface (DFI) on a digital line trunk unit (DLTU) shelf. On an SM-2000, entry is also possible as a DS0 channel embedded in a SONET terminating equipment facility terminated on a resident transmission multiplexer (TMUX) on a digital networking unit - SONET (DNU-S).

When CCS signaling links (CCSLKs) are provisioned and activated, time slots are automatically nailed-up from the access equipment through the timeslot interchange (TSI) unit and data fanout (DF), to provide a dedicated connection to a signaling terminal protocol handler (ST PH) in the packet switch unit (PSU).

- The ST PH can physically terminate up to four CCSLKs (the number depends on office engineering guidelines). The ST PH provides the SS7 message transfer part (MTP) physical and data link layers for the links. See "SS7 Protocol Definition," Section 12.1.5, for a detailed description of the MTP protocol specifications. The ST PH is physically a protocol handler version 3 (PH3) installed on a PSU1/PSU2 (PSU version 1/2) shelf, with a new image dedicated to SS7 functionality.

Most of the SS7 MTP network layer services, as well as applications layer user services, are provided in the switch module processor (SMP). Therefore, transport between the ST PH and SMP is required:

- Incoming signaling messages, called message signaling units (MSU), arrive at the ST PH, through the nailed-up path from the signaling data link (SDL) access equipment. Then they are transported to the SMP directly through the packet fanout (PF), control fanout (CF) and packet interface version 1 or 2 (PI/PI2) on the resident switching module processor (SMP).
- Outgoing MSUs originating in the SMP must use a message delivery protocol handler (MD PH) for distribution to the appropriate signaling terminal protocol handler (ST PH). When messages arrive at the appropriate ST PH, they are delivered to the target SDL, through the nail-up connection.
- The MD PH terminates an intra-SM MD link, which is actually an implicit "link" between the MD PH and the SMP, to distribute outgoing MSUs that originate in the SMP. MSUs are delivered from the SMP to the MD PH, through the PI/PI2-CF-PF path, and are then forwarded to the appropriate ST PH through the PF.

As CCSLKs may be terminated on different ST PHs, proper routing is provided by the MD PH, to offload SMP resources. This function is critical to all CCS operations in the GSM.

The intra-SM-MD link may be combined with CCSLK terminations on the *same* PH, if office engineering guidelines allow this configuration.

ISUP trunk routes can be defined, as in any 5ESS[®]-2000 switch office. This includes analog voice/data trunks terminated on an equipped trunk unit (TU) circuit, or digital trunks on a 56 Kbps or 64 Kbps DS0 channel on an equipped DFI facility. On an SM-2000 switch office, digital trunks may also be terminated on a DS0 channel on a DNU-S STE facility. The only restriction is that ISUP trunks using GSM-based SS7 signaling must terminate on that GSM.

12.1.3 GSM Terminology and Signaling Link Configurations

This section introduces signaling terminology for a global switch module (GSM), and describes possible signaling configurations.

- **GSM** - A global SM is simply an SM/SM-2000 that contains a PSU platform that terminates CCS signaling links (CCSLKs). In the 5E11 software release, only a 5ESS®-2000 switch VCDX could be provisioned as a GSM; in the 5E12 software release, in addition to VCDXs, up to 16 SM/SM-2000s in a 5ESS®-2000 switch may be provisioned as GSMs.
- **point codes** - Point codes are used in signaling messages to uniquely define exchanges/STPs in the CCS network. From the perspective of the GSM, these point codes are defined:
 - **OPC** - An originating point code (OPC) is provisioned to identify a GSM. In the 5E12 software release, when multiple GSMs can exist on the same 5ESS®-2000 switch, each GSM must have a unique OPC, which is also different than the OPC or aliases for a common network interface (CNI), if equipped.
 - **APC** - An adjacent point code (APC) is the far-end exchange/STP that *directly* terminates CCSLKs emanating from the GSM.
 - **DPC** - A destination point code (DPC) is any exchange/STP that terminates either CCSLKs or trunk routes directly, or other destinations within the regional network that contains data bases for special services. Up to 2000 DPCs may be defined for a GSM, but only 255 DPCs (in the 5E11 software release) or 1024 DPCs (in the 5E12 software release) that directly terminate trunk routes may be defined.

NOTE: In the 5E11 software release, only point codes in ANS® format are allowed. In the 5E12 software release, OPC/DPCs in the AT&T network (network 254) or UNITEK network (network 236) are represented in AT&T format. See the APP-POINT CODE appendixes in the 235-600-700, 5ESS®-2000 Switch Input Message Manual and the 235-600-750, 5ESS®-2000 Switch Output Message Manual for format details.

- **CCSLK** - A CCS signaling link (CCSLK) is a 56 kilobit or 64 kilobit signaling connection between the GSM and other point codes. (See "PSU Hardware Platform," Section 12.1.2, for a detailed description of the hardware architecture within the GSM.) Up to 32 CCSLKs may be defined on a GSM.
- **LS** - A link set (LS) is a grouping of link members (CCSLKs) that terminate on the same APC. A link set consists of up to 8 link members prior to the 5E14 software release, and up to 16 link members in the 5E14 and later software releases. When a link set is provisioned as the signaling route to a DPC, signaling messages to the DPC are distributed (load shared) over the active links in the link set. Up to 16 LSs may be defined in for a GSM.
- **CLS** - A combined link set (CLS) is another logical grouping that may be defined to load share over diverse routes (such as a mated pair of regional STPs). A CLS is composed of two LSs (usually to different APCs), and signaling messages assigned to depart on a CLS are distributed among CCSLKs in both LSs. On a GSM, up to 8 CLSs may be defined, but a given LS may be a member of only one CLS.
- **DPC route sets** - For a given DPC, a normal (primary) LS/CLS plus up to four alternate LS/CLSs, may be defined for signaling message transport. If signaling messages are destined for a particular DPC, CCSLKs in the normal (primary) LS/CLS are used, if at least one member CCSLK is available for transport. If all CCSLKs in the normal (primary) LS/CLS are unavailable due to GSM or network problems, an alternate LS/CLS (in the order specified in the office dependent data [ODD]) is used. This process can be repeated with other alternate LS/CLSs, if the chosen alternate LS/CLS become unavailable, until there are no more alternates defined. The group of normal plus alternate LSs/CLSs is the route set for a DPC.
- **Load Sharing and SLSs** - Messages are distributed over the active links in the current route (LS or CLS) by means of signaling link selectors (SLS). Each LS has 16 SLSs and each CLS has 32 SLSs divided among the active links in the LS or CLS, respectively. The user or application parts assign an SLS to each message and all messages with the same SLS are sent over the link currently assigned to carry that SLS. This ensures that

messages that are part of the same call or transaction are delivered in sequence.

- **SLT** - A sequence of sending an MTP level 3 test message signaling unit on a CCSLK and receiving an acknowledgment, which verifies link integrity, is called a signaling link test (SLT). An SLT is executed before a CCSLK can be successfully restored, is executed periodically on active, noncongested CCSLKs, and can be manually initiated. In 5E13 and later software releases, SLTs are also periodically executed on congested CCSLKs, and periodic SLTs can be manually inhibited (via a secured feature).

12.1.4 NGSM and CMT Terminology

Two terms introduced for 5E14 and later software releases are:

- **Non-global SM (NGSM)** — A non-global SM is an SM that serves ISUP/TCAP clients, and must use an SS7 PSU platform on a GSM for signaling to the external CCS network. A GSM can support resident ISUP/TCAP clients (in other words, a GSM can provide NGSM functionality). In the 5E14 software release, the GSM is its only permissible NGSM; this constraint is relaxed in later software releases.
- **CCS Message Transport (CMT)** — CCS message transport is an internal 5ESS®-2000 switch messaging mechanism used to transport CCS messages moving between ISUP/TCAP clients on an NGSM to the associated SS7 PSU platform on a GSM.

In 5E14, CMT is restricted to intra-SM message delivery transport; this constraint is generalized in later software releases.

Switch personnel can view connectivity from the GSM or NGSM perspective, but because of the 5E14 constraint that the only permissible NGSM is its associated GSM, the information presented is identical.

12.1.5 SS7 Protocol Definition

The GSM satisfies the SS7 protocol specifications for a signaling end point (SEP) office, defined in accordance with standards established by the American National Standards Institute (ANSI®).

The SS7 protocol model supported includes the message transfer part (MTP), which is the hardware/software used to transfer messages between two CCS signaling points, and the signaling connection control part (SCCP), which is used for non-circuit related message transfer. The MTP and SCCP functions are:

- **MTP level 1** provides the physical medium for the transmission of the signaling bit stream, using the GSM's SS7 PSU hardware described in "PSU Hardware Platform," Section 12.1.2. This includes the 56Kbps/64Kbps digital transmission provided by the signaling data link (SDL) on through to the appropriate signaling terminal protocol handler (ST PH) on the GSM's PSU.
- **MTP level 2** functions ensure reliable transmission over the signaling data link (SDL) between two signaling points. While the SDL and intra-SM nailed-up path to the ST PH provide the physical/electrical path to carry the data bit-stream, the high level data link control (HDLC) terminating hardware and software in the ST PH provide level 2 functions. This includes signaling unit (SU) delimitation, alignment, signaling link error monitoring, error detection and correction, and flow control.
- **MTP level 3** transfers data transparently between end users in different exchanges. In the GSM, this function is generally shared by the SMP and ST/MD PHs and is composed of two major categories:
 - **Signaling message handling** functions ensure that message signal units (MSUs) originated by a user in one point code are delivered to the intended destination user in the DPC designated by the originator. Signaling message handling includes routing of outgoing MSUs and discrimination and distribution of

incoming MSUs.

The *routing function* determines the CCSLK to use for GSM-originated messages based on the DPC and SLS.

The *discrimination function* determines whether an incoming message is destined for the office at which it arrived based on the DPC in the message. Because a GSM does not have STP functionality, incoming messages not destined or the GSM's OPC are discarded.

The *distribution function* relays incoming messages, that survive discrimination, to the appropriate higher layer (SCCP in the PH, ISUP in the SMP or network test and maintenance functions in the SMP) based on the service indicator in the MSU.

- **Signaling network management** functions provide reconfiguration of the signaling network in case of failure and recovery, and control traffic in case of congestion. Signaling network management functions include signaling traffic management, signaling link management and signaling route management.

Signaling traffic management functions include changeover, changeback and congestion control. Changeover moves traffic from a link or route that is about to be removed to another link or route. Changeback moves the traffic back when the link or route again becomes available.

Signaling link management functions control CCSLK activation/deactivation, blocking/unblocking, and inhibiting/uninhibiting.

Signaling route management functions provide information to signaling traffic management on the availability, unavailability, and congestion levels of signaling routes.

- **SCCP** (signaling connection control part) allows for a user to transfer circuit and non-circuit related information between the GSM and specialized centers in the CCS network (such as an NCP or SCP or LASS services), using logical signaling connections. It is used primarily to support transaction capabilities user part (TCAP) features.

The connectionless SCCP provides the ability to route messages based upon a global title translation (GTT). During GTT, the address of a global title (such as an 800 number and transaction type) is translated to a physical DPC. Using connectionless SCCP, the subsystem number (SSN) does not have to be known.

See "Signaling System 7 (SS7) Overview," Section 2, of this document for detailed information about basic SS7 protocol attributes.

Because CCSLK access and all levels of MTP/SCCP, ISUP trunk terminations, as well as call processing software, are self-contained within the GSM, the loss of connectivity with the AM/CM does not affect call processing (if stand-alone call processing is provisioned) or autonomous maintenance activities of the CCS network.

12.1.6 ISDN User Part Services Provided

Integrated services digital network user part (ISUP) definition provides the GSM with signaling system 7 (SS7) protocol requirements to support basic bearer services and supplementary services for voice/non-voice applications. Prior to the 5E11 software release, these services were available only with a CNI signaling platform, but in 5E11 and later releases, many of these capabilities are available on GSMs provisioned for PSU-based signaling.

The ISUP services include:

- Trunk signaling is the most significant feature of ISUP. This includes standard common channel signaling 5ESS[®]-2000 switch call processing features available through the current software release.

For details on each feature see the appropriate section in this document.

Section 5.2	Normal call setup, connect and release of ISUP trunks.
Section 5.3	Call setup enhancements.
Section 5.4	Q.931/ISUP interworking and supplemental bearer services.
Section 9	ISDN User-Network Interface and ISUP Interworking.
Section 10	Signaling end point (SEP) applications of ISUP Network Interconnect.
Section 11.12	ISUP interworking support for fractional DS1 services terminated on a GSM-resident
	primary rate interface (PRI).
Section 11.14	ISUP support for interswitch voice messaging service (ISVM).

- The ISUP messaging set supports the interface between the trunk port status administration and testing in the GSM, and coordinating with the far-end switch (and visa-versa). This includes the following attributes, described in "Trunk Maintenance," Section 5.8, and "Voice Path Assurance Test Consideration," Section 5.9, in this document.

Section 5.8.3	Machine detected inter-office irregularity (MDII) reporting.
Section 5.8.4	Blocking and unblocking activity (both sending and receiving, both individual trunk and circuit group messages).
Section 5.8.5	Automatic continuity check/recheck.
Section 5.8.6	Reset (both sending and receiving, both individual trunk and circuit group messages).
Section 5.8.7.1	Manual/automatic trunk query, ensuring synchronization of near-end and far-end call processing and maintenance states.
Section 5.8.8	Manual circuit validation testing, ensuring near-end and far-end ISUP trunk office dependent data (ODD) consistency.
Section 5.8.9	Manual/automatic ISUP trunk testing, by incoming/outgoing test calls.
Section 5.8.10	Trunk line and work station (TLWS) interfaces for ISUP trunks.
Section 5.9	Voice path assurance test.

A major difference between 5ESS®-2000 switch CNI-supported offices and SM-based SS7 services on a GSM occurs during SM initialization or entry/exit from SM isolation; see Section 5.8.11 for a description of the CNI environment. Because CCS signaling in the GSM is wholly self-contained on the SM's packet switch unit (PSU) platform and peripheral access hardware, there are differences in the availability of CCS services. In the GSM:

- Blocking messages are not sent to far-end offices when the GSM enters full initialization, because the CCS signaling interface (SM-resident) is not available when the SM initializes. After the initialization completes, reset messages (on a circuit group basis, if possible) resynchronize trunk status.
- Blocking messages are not sent to far-end offices when the GSM enters selective initialization, but transient calls are torn down (stable calls are not impacted); new call set-ups fail for the duration of the initialization. After the initialization completes, reset messages resynchronize trunk status for ISUP trunks where transient calls have been disrupted; other trunks are instantly available (unblocking/blocking messages are sent as a refresh mechanism in the 5E12 software release).
- Blocking messages are not sent as the GSM enters isolation, nor are unblocking messages sent as the GSM exits isolation. Because the CCS platform is self-contained in the GSM and call-processing uses local hunting, entry/exit into SM isolation has no effect upon ISUP call processing or most maintenance activities. No maintenance personnel requests involving the SM are accepted during SM isolation.

12.1.7 Transaction Capabilities Application Part Services Provided

The transaction capabilities application part (TCAP) feature provides the GSM with signaling system 7 (SS7) protocol requirements to support many specialized applications. Prior to the 5E11 software release, these services were available only with a CNI signaling platform, but in 5E11 and later software releases, many of these capabilities are available in GSMs provisioned for PSU-based signaling.

The following applications are supported on a GSM, with the restriction that TCAP features are only supported with

respect to signaling end point (SEP) offices.

- The service switching point (SSP) feature is provided to support 800 number services, as described in "SSP 800 Number Service Feature," Section 11.8 .
- Local area signaling service (LASS) is supported in 5ESS®-2000 switch VCDX offices. LASS features are described in "Local Area Signaling Service Features," Section 11.10 , and a more detailed description/customer interface with LASS can be found in 235-190-130, *Local Area Signaling Services Feature*. These individual LASS features are supported:
 - Automatic callback
 - Automatic recall
 - Customer-originated trace
 - Individual calling line identification
 - Screen list editing
 - Selective call acceptance
 - Computer access restriction
 - Selective call forwarding
 - Selective call rejection
 - Selective distinctive alerting.
- The interswitch voice messaging (ISVM) transaction capabilities application part (TCAP) services are supported, as described in "Interswitch Voice Messaging Service," Section 11.14 .
- Advanced services platform (ASP) release 0.1B features are available on VCDX GSMs in a 5E11 software update; release 0 is not available on a VCDX GSM. Both release 0 and 0.1B are available on 5ESS®-2000 switch GSMs beginning in the 5E12 software release. See "Advanced Services Platform (ASP)," Section 11.7 for a brief overview, or refer to one of these documents for details:
 - 235-190-125, *Advanced Services Platform Release 0 and 0.1A Features*
 - 235-190-126, *Advanced Services Platform Release 0.1B Features*
 - 235-030-100, *Advanced Services Platform Network Architecture and Service Consideration Guide*.
- The Local Number Portability (LNP) service, which is a capability supported by the advanced services platform, is available on VCDX GSMs in a 5E11 software update, and on 5ESS®-2000 switch GSMs beginning in the 5E12 software release. Refer to one of these documents for details:
 - 235-190-127, *Number Portability User's Guide*
 - 781-610-300, *Number Portability Roadmap*
- TCAP test queries for LASS services, NS800 services, and ASP are provided in all GSM environments beginning in the 5E12 software release, noting that the OPC of the CNI/GSM may be specified to target specific

SS7 platforms.

- Direct signaling event (DSE) traps for NS800 services, ISVM, and ASP are provided in all GSM environments beginning in the 5E12 software release.

It should be noted that all operator services position system (OSPS) services and network management control are **not** supported in GSM environments.

12.2 USER OPERATION

12.2.1 Introduction

The following subsections define CCS-related states, Master Control Center (MCC) pages, status access and manual reconfigurations, which are used for GSM administration and maintenance.

See "Feature Implementation," Chapter 13, for detailed provisioning procedures and "Maintenance Considerations," Chapter 14, for CCS trouble clearing procedures.

It should be noted that all administrative and maintenance features cited are applicable to 5ESS®-2000 switch VCDX environments in the 5E11 software release, and to both VCDX and 5ESS®-2000 switch SM/SM-2000 environments in the 5E12 software release, unless stated otherwise. Modifications or additional capabilities specifically cited as 5E12 developments are available in all environments, but only for offices using that software release.

12.2.2 GSM SS7 States

The local operation of a GSM depends upon:

- CCS signaling links (CCSLKs)
- Signaling data links (SDLs)
- Link sets (LSs)
- Intra-SM message delivery (MD) link.

The status of these maintenance entities is important to the health of a CCS operation. It is necessary to know when the operation of these entities is disrupted by automatic recovery procedures or manual actions, in order to effectively handle administrative provisioning procedures or perform maintenance trouble clearing actions.

CCS signaling link (CCSLK) states are described in Table 12.2-1. The states are composite conditions (primary port status, inhibit/blocking information, congestion data) of that link.

Table 12.2-1 CCSLK States in a GSM

STATE	DESCRIPTION
ACT	The CCSLK is active, able to carry traffic, if it is not inhibited or blocked. Many status reports specify CCSLKs are available (AVAIL), rather than the ACT state displayed on the MCC. Message Transfer Part (MTP) blocking, inhibit and congestion information provide qualifications: LBLK - Locally blocked indicates that the GSM restricts all traffic on a specific link (it sends continuous status indicator processor outages [SIPOs] to the remote switch). RBLK - Remotely blocked indicates that the remote switch restricts all traffic on a specific link (the GSM receives continuous SIPOs from the remote switch). LINH - Locally inhibited indicates that the GSM only transmits and receives test or maintenance messages, but neither end may use the link for normal signaling associated with call processing. Inhibiting requires negotiation, i.e., message/acknowledgment handshake, with the remote switch. RINH - Remotely inhibited indicates that the remote switch only transmits or receives test or ISUP maintenance messages, but neither end may use the link for normal signaling associated with call

	processing (this requires negotiation, i.e., message/acknowledgment handshake, with the GSM). CONG1 - The link is ACT, but first level MTP congestion thresholds have been exceeded, and least severe level 2 traffic throttles are in effect. Application of congestion control/changing message traffic patterns should eventually relieve this problem. CONG2 - The link is ACT, but second level MTP congestion thresholds have been exceeded, and intermediate level 2 traffic throttles are in effect. Application of congestion control/changing message traffic patterns should eventually relieve/reduce this problem. CONG3 - The link is ACT, but third level MTP congestion thresholds have been exceeded, and most severe level 2 traffic throttles are in effect. Application of congestion control/changing message traffic patterns should eventually relieve/reduce this problem. NOTE: The LBLK, LINK, and RINH qualifiers may be applied to a non-ACT CCSLK, but have no meaning until the CCSLK is activated. The RBLK qualifier can only occur on an ACT CCSLK.
INIT	The CCSLK is awaiting initialization, typically occurring after a GSM full initialization, or as a result of audit recovery. This link is eventually elevated to an ACT state, or, if the initialization fails, makes a transition to a more specific out-of-service (OOS) state.
LKER-L3	An MTP level 3 protocol link test error has occurred (probably an ODD error, or switched wire at the T1 patch panel). Transient failures are resolved automatically by periodic attempts to re-execute the link test.
LKER-L2	A MTP level 2 error indicates a failure to align a link, possibly due to undetected PH/facility failure, or a problem at the APC. Transient failures on transmission facilities are resolved automatically by periodic attempts to realign the link.
LKER-L1	The MTP level 1 path for the signaling link cannot be established, a rare case that may occur in non-SM-2000s, where there are no available network timeslots, or in any GSM where ODD corruption results in overengineering of PSU timeslots. Transient failures are resolved automatically by periodic attempts to reinitialize the link/path.
RSRC	The CCSLK is OOS "due to lack of internal switch resources" (failure of software to gain ownership of a CCSLK to perform maintenance actions, inability to link data structures, inability to read related ODD data, dynamic related data, inability to send a message and/or a lost message, etc.). Transient occurrences are resolved automatically by periodic attempts to reinitialize the link/internal path.
OOST	The CCSLK is out-of-service (OOS) on a transient basis (state change is occurring, as controlled by a maintenance process, and will be stable shortly). A subclass to-be-idled (TBI) is used by audit recovery; the port is inaccessible to maintenance software until automatic recovery completes. This additional information is provided by the OP:STATUS,CCSLK request, but not on MCC displays.
OOS-DL	The CCSLK is out-of-service (OOS) for "family-of-equipment" reasons. Its associated signaling data link (SDL) port is OOS due to manual SDL trunk removal, detected parent DFI/DNU-S hardware failure or manual removal, or associated facility failure. The underlying SDL or its parent access hardware/facility must be restored before any attempt is made to reinitialize the signaling link.
OOSF-PH	The CCSLK is OOS for "family-of-equipment" reasons. Its parent channel group is unassigned due to PH faults or PH manual removal. The underlying channel group must be assigned before any attempt is made to reinitialize the signaling link.
DACT	The CCSLK has been manually deactivated (removed from service). The link must be manually activated to return it to service.

There may be multiple conditions that cause a CCSLK to be unavailable, such as simultaneous manual deactivation and a faulty PH. In this example, the most severe condition (DACT) is illustrated. If the CCSLK is manually restored, the secondary condition (OOSF-PH) dominates.

Signaling data link (SDL) states are described in Table 12.2-2. The SDL represents the GSM access for the CCSLK, but it is also a trunk port and possesses an independent state. SDL states listed in Table 12.2-2 are in the standard form used in output messages (base state - qualifier - operational restriction).

Table 12.2-2 SDL States in a GSM

STATE	DESCRIPTION
IS	The SDL is in-service (this only refers to the availability of the DFI/DNU-S trunk port used by the CCSLK for external access, not the usefulness of the link itself in CCS operation)
OOS-MTCE-DSBLD	The SDL port has been manually removed; the port must be restored manually. The parent CCSLK is not functional.
OOS-MTCE-FAF	The SDL port is OOS due to a carrier group alarm (CGA) on its associated DFI/DNU-S facility; this SDL port status is deleted automatically when the CGA clears. The parent CCSLK is not functional.
OOS-MTCE-FE	The SDL port is OOS due to "family-of-equipment" reasons, i.e., parent DFI/DNU-S access hardware, or an associated facility, has been removed (excludes facility failures due to a CGA). The parent CCSLK is not functional.

SDL states may exist simultaneously: for example, an OOS-MTCE-FE condition (due to parent hardware removal), plus OOS-MTCE-DSBLD (due to a simultaneous manual removal). Both primary and pending states may be viewed by using the `OP:STATUS` input message with the appropriate digital equipment number (DEN) or network equipment number (NEN) as an identifier.

Link set (LS) states are described in Table 12.2-3. The summary LS states displayed on the 1532 MCC display page are derived from the most severe CCSLK status for a link in that LS. The states listed in Table 12.2-3 are listed in order of severity, the more severe conditions appear at the bottom of the list. A **red** background color on the LS status displayed on the 1532 MCC display page indicates **all** member CCSLKs are unavailable for CCS use.

Table 12.2-3 Summary LS States in a GSM

STATE	DESCRIPTION
GROW	No member CCSLKs provisioned (but LS exists)
ACT	All member CCSLKs in the LS are ACT
CONG	At least one member CCSLK is experiencing congestion (level 1/2/3)
INIT	At least one member CCSLK is initializing
RINH	At least one member CCSLK is remotely inhibited
LINH	At least one member CCSLK is locally inhibited
RBLK	At least one member CCSLK is remotely blocked
LBLK	At least one member CCSLK is locally blocked
RSRC	At least one member CCSLK is OOS due to resource problems
OOST	At least one member CCSLK is changing state (transient)
LKER	At least one member CCSLK experienced a link error (level 1/2/3)
OOSF	At least one member CCSLK is OOS for "family of equipment" reasons (parent PH channel group is unassigned, or SDL is OOS)
DACT	At least one member CCSLK is manually deactivated

Intra-SM message delivery (MD) link states are described in Table 12.2-4.

Table 12.2-4 Intra-SM MD Link States

STATE	DESCRIPTION
ACT	The intra-SM MD link message distribution capability is functioning normally (active).
INIT	The intra-SM MD link is OOS on a transient basis; a state change is occurring, and will be stable shortly.
OOSF-PH	The intra-SM MD link is OOS for "family-of-equipment" reasons. The associated channel group is unassigned, due to a detected PH failure. The channel group must be reassigned before initialization of the intra-SM MD link is attempted.
DACT	The intra-SM MD link has been manually removed and must be manually restored to service.
LKER	The intra-SM MD link is awaiting initialization, typically after a GSM full initialization, or as a result of audit recovery. This MD link is eventually elevated to an ACT state (periodic initialization attempts are scheduled automatically), unless initialization fails. NOTE: In 5E14 and later software releases, the LKER state is eliminated. The functionality described is incorporated in the INIT state.

12.2.3 Master Control Center Overview

To maintain the CCS aspects of a GSM with the PSU platform, some new master control center (MCC) display pages have been added and some existing pages have been modified.

See 235-105-110, *5ESS®-2000 Switch System Maintenance Requirements and Tools* for a complete description and illustration of MCC display pages. These MCC pages are used to maintain a GSM:

- *141-144 EQUIPPED SM STATUS SUMMARY* MCC pages were modified in the 5E12 software release to add the prefix **G** to the existing SM type displayed. This identifies office GSMs.
- *1180-1184 PSU 0 SHELF 0-4* MCC pages are used to determine if CCS channel groups are provisioned, and if they are currently being served by an active PH. The channel group types of interest are
 - MD (intra-SM MD link functionality only)
 - ST7 (CCSLK terminations only)
 - MDST7 (both CCS functions served by the same PH).
- *1010 SM STATUS* MCC page added two indicators. The string "SEE PAGE 1532" always appears if CCS functionality is equipped. The indicator is back lighted (red background) if CCSLKs become off-normal. Another back lighted indicator "SEE PAGE 1530," appears only if the intra-SM MD link is off-normal.

Two SM status phases have been added to highlight CCS-related problems:

- **CCSLKOFFN** indicates one or more CCSLKs are off-normal.
- **CCSMDOFFN** indicates the intra-SM MD link is not active.

In 5E14 and later software releases, **CCSMDOFFN** is replaced by more general phases:

- **CMT_LOST** indicates all internal CMT connectivity on the GSM is unavailable (in 5E14, implies that the intra-SM MD link is not ACT).
- **NCMT_LOST** indicates all internal CMT connectivity on the NGSM is unavailable (in 5E14, also implies that the intra-SM MD link is not ACT because the NGSM must be the GSM itself).
- *1530 MESSAGE DELIVERY STATUS* MCC page provides status for the intra-SM MD link and the PH channel group termination of that link. A non-active intra-SM MD link results in cessation of *all* CCS-supported ISUP/TCAP activity on the GSM. Menu selections on this MCC page allow activation or unconditional deactivation of the MD link and output of MD link status to the ROP.

In 5E14 and later software releases, the *1530* MCC page is eliminated. The equivalent status information is provided on the *1540* MCC page.

- *1532 CCS LINK SET SUMMARY* MCC page provides summary status for every LS provisioned on a GSM. This information is useful during provisioning activities, as well as determining the "health" of an entire LS. Menu selections allow activation/unconditional deactivation of all members of a specified LS or generation of detailed status output for all members of the LS.
- *1533 CCS LINK SET MEMBER STATUS* MCC page provides detailed status for *each* CCSLK in a specified LS (including local/remote blocking/inhibit and congestion status), and convenient mappings to DFI/DNU-S access

equipment numbers and PSU channel group assignments. Menu selections allow reconfiguration of a specific CCSLK (including activation/deactivation, inhibit/uninhibit, block/unblock, test actions), and the ability to output a detailed status report for a given CCSLK.

- 1540 GSM CMT STATUS MCC page provides details of internal CCS message transport (CMT) on a GSM (available in 5E14 and later software releases). This page provides an instant view of CMT accessibility to all supported NGSMs via status boxes (*GREEN* backlighting for an accessible NGSM, and *RED* backlighting for an inaccessible NGSM). Menu selections allow detailed NGSM CMT status or intra-SM MD link status to be output to the ROP, or detailed CMT status to be displayed on the bottom of the MCC page.

In the 5E14 software release, the only NGSM provisionable is the GSM itself, and CMT transport must use the intra-SM MD link. All data provided on the 1540 MCC page refers to intra-SM MD link transport.

- 1541 NGSM CMT STATUS MCC page provides details of internal CCS message transport (CMT) on an NGSM (available in 5E14 and later software releases). This page provides an instant view of CMT accessibility associated with the NGSM to all supported GSMs via status boxes (*GREEN* backlighting for an accessible GSM, and *RED* backlighting for an inaccessible GSM). Menu selections allow detailed GSM CMT status or intra-SM MD link status to be output to the ROP, or detailed CMT status to be displayed on the bottom of the MCC page.

In the 5E14 software release, the only GSM provisionable is the NGSM itself, and CMT transport must use the intra-SM MD link. All data provided on the 1541 MCC page refers to intra-SM MD link transport.

12.2.4 Status Query

Useful status reports and miscellaneous mappings are available by using input message requests for these CCS entities:

- CCS signaling links (CCSLKs)
- Signaling data link (SDL) ports
- Link sets (LSs) or combined link sets (CLS)
- Intra-SM message delivery (MD) link
- Destination point codes (DPCs) or adjacent point codes (APCs)
- CCS message transport (CMT), in 5E14 and later software releases.

The following list describes input and output messages for these entities. See the 235-600-700, *5ESS®-2000 Switch Input Message Manual* and the 235-600-750, *5ESS®-2000 Switch Output Message Manual* for detailed descriptions. Messages in these documents are organized alphabetically by message ID, shown here.

- **OP:ST-CCSLK** generates a detailed status report for an individual CCSLK on a specific GSM (including detailed OOS CCSLK status, local/remote inhibit/blocking information, and congestion data) and PSU/access equipment number (if the CCSLK is active). By using input options, the search can be restricted to available/unavailable CCSLKs or a single input request can produce the status for multiple members in one or more LSs.
- **OP:CCS-ACTLK** lists the *number* of active CCSLKs in each LS on a specific GSM.
- **OP:CCS-GSM** provides a high-level indication if the GSM is defined or not. If the GSM is defined, this message shows if all CCSLKs on a GSM are active, or if one or more CCSLKs are off-normal. If a specific GSM is not specified, status of all GSMs in the office are produced.

In 5E14 and later software releases, the status of CMT connectivity associated with a GSM is also provided.

- `OP:CCS-SLS` provides signaling link selector (SLS) values that show traffic distribution. The output may be restricted to CCSLKs in a given LS/CLS, or to links currently carrying traffic to a given DPC (as specified in an input message parameter). Both the *normal* SLS distribution (what should occur, if all related CCSLKs are active), and *current* SLS distribution (actual SLS distribution, which accounts for unavailable CCSLKs) are produced as output.
- `OP:ST-MD` provides intra-SM MD link detailed status for a specific GSM, as well as PSU terminating data.
- In 5E14, the generalized concept of internal CCS message transport (CMT) is introduced, and the following status commands are available:
 - `OP:ST-GSMNET` provides CMT status for NGSMs associated with a specified GSM.
 - `OP:ST-NGSMNET` provides CMT status for GSMs associated with a specified NGSM.

In the 5E14 software release, the only NGSM provisionable is the GSM itself, and CMT transport must use the intra-SM MD link. All data provided by these commands refers to intra-SM MD link transport.

- `OP:CCS-CLS` provides the status of all CCSLKs belonging to the specified CLS on a GSM; this includes primary status, as well local/remote inhibit/blocking data, for each child CCSLK, and the number of SLS values assigned to that link.
- `OP:CCS-LSCLS` provides a mapping of links sets to the CLSs on a specific GSM (if any) to which they belong. One link set or a range of link sets may be specified in the input. If no link set is specified, the output produced is for all LSs equipped on the specified GSM. Each link set can map to only one CLS.
- The following messages determine the general availability of DPCs served by a specific GSM, and produce mapping information to the CLS/LS currently carrying traffic to the DPC.
 - `OP:CCS-ACDPC` lists the LS/CLS *currently serving* each *accessible* DPC served by the specified GSM; this is the *normal* (primary) LS/CLS defined in ODD under fault-free conditions, but may be an alternate LS/CLS if the normal LS/CLS is unavailable.
 - `OP:CCS-DPCLS` lists DPCs *currently* being served by a specified LS/CLS; this list does not include DPCs, that have the designated LS/CLS specified as an *alternate* route, when it is not being used for access.
 - `OP:CCS-DPC` produces accessibility, inaccessibility, or congestion data for one or more DPCs on a specific GSM, and the LS/CLS currently used to access each DPC specified if it is accessible.
- The following messages report state transitions and inaccessible conditions.

A `REPT CCSLK` message is produced when the CCSLK makes a state transition due to automatic recovery or manual action. The basic availability/unavailability of the link is specified, along with qualifiers providing more detailed status information; if the CCSLK is restored, the resultant parent PSU/access equipment numbers are provided. If a CCSLK fails autonomously, this message is important because it provides reasons for link failure and major alarm (in addition to status information).

A `REPT MD` message is produced when the intra-SM MD makes a state transition, due to automatic recovery or manual action. Due to the critical nature of the intra-SM MD link, this message may specify the reason for autonomous removal (removal due to automatic recovery causes the message to be critically alarmed, and this alarmed message is repeated periodically because of the seriousness of the problem). In 5E14 and later

software releases, this message is no longer alarmed, and a more generalized report of CMT status changes is provided.

A REPT CCS MESSAGE TRANSPORT CONNECTIVITY CHANGE message is produced in 5E14 and later software releases. This message is produced when CMT connectivity between a GSM and one or more NGSMs becomes accessible or inaccessible. If inaccessibility occurs because of automatic recovery, the message is critically alarmed (and if all CMT connectivity to a GSM is lost, the alarmed message is repeated periodically). In the 5E14 software release, the only NGSM provisionable is the GSM itself, and CMT transport must use the intra-SM MD link; all data provided by this report refers to intra-SM MD link transport.

A REPT CCS-APC message is produced when an APC becomes inaccessible due to manual or automatic action. This message is critically alarmed regardless of the cause. A similar message is also produced when the APC becomes accessible (no alarm).

A REPT CCS-DPC message is produced if one or more DPCs becomes inaccessible to a specific GSM. Normally the message is accompanied by a major alarm, but a critically-alarmed message is produced if *all* DPCs become inaccessible, indicating a specific GSM is completely isolated from a CCS perspective. In the 5E12 software release, a similar message is also produced when the DPC becomes accessible (no alarm).

- In 5E13 and later software releases, the GSM PSU signaling platform supports operation, maintenance and administration part (OMAP) functionality. The GSM originates MTP Routing Verification Test (MRVT) and SCCP Routing Verification Test (SRVT) messages, intended to verify the routing data in the SS7 network as it pertains to the GSM.

Provisioning aspects are discussed in Section 13.1.22, and a detailed user's guide for OMAP functionality is presented in Section 12.5.3.

12.2.5 Manual Reconfigurations

Sometimes during the administration or maintenance of a GSM, it is necessary to reconfigure these CCS entities:

- Signaling links (CCSLKs)
- Intra-SM message delivery (MD) link
- Signaling data link (SDL) ports
- Parent protocol handler 3 (PH3) hardware
- Parent digital facility interface (DFI) or digital network unit - SONET (DNU-S) hardware/facilities

The following list describes input and output messages for these entities. See the 235-600-700, *5ESS®-2000 Switch Input Message Manual* and the 235-600-750, *5ESS®-2000 Switch Output Message Manual* for detailed descriptions. Messages in those documents are organized alphabetically by message ID, shown here.

- **RMV:CCSLK** manually removes a specified CCSLK (either complete deactivation, or to inhibit/block the link locally, as specified in an input parameter).

Sufficient protection exists to ensure that the CCS operation is not severely affected by *deactivation* (only 50% of the equipped CCSLKs in a LS may be conditionally deactivated), but an unconditional option is available for ultimate manual control. The last active CCSLK serving any DPC cannot be inhibited even with an unconditional option. However, inexperienced personnel should be careful when using *blocking*, because it is always treated as unconditional, and can cause inaccessibility to other offices.

Appropriate range specifications in a single input request can remove multiple CCSLKs in one or more LSs on a specific GSM.

- **RST:CCSLK** manually activates, uninhibits or unblocks a CCSLK (the state condition to be deleted must be specified).

Appropriate range specifications in a single input request can restore multiple CCSLKs in one or more LSs on a specific GSM.

- **TST:CCSLK** manually initiates a signaling link test (SLT) on a specified CCSLK.

Appropriate range specifications in a single input request can test multiple CCSLKs in one or more LSs on a specific GSM.

- CCSLK reconfigurations are available with menu selections on the *1533 CCS LINK SET MEMBER STATUS* MCC page for a specific GSM. These useful pokes are summarized in Table 12.2-5.

NOTE: "xx" is the CCSLK member number in the LS displayed.

Table 12.2-5 1533 MCC Page CCSLK Reconfiguration Menu Commands

COMMAND	ACTION	RECONFIGURATION ACTION
2xx[UCL]	Deactivate	Deactivate or remove a CCSLK from service
3xx	Activate	Activate or restore a deactivated CCSLK to service
6xx	Inhibit	Inhibits CCSLK (only test/maintenance messages allowed)
7xx	Uninhibit	Restores a locally inhibited CCSLK to service
62xx	Block	Blocks CCSLK (no message traffic allowed)
72xx	Unblock	Restores a locally blocked CCSLK to service
5xx	Test	Executes MTP Level 3 test on CCSLK

When using these reconfiguration menu selections (pokes):

- No other qualifiers (other than the UCL qualifier on the 2xx poke) may be appended to the menu selection inputs described.
- The 2xx (deactivate CCSLK) menu selections generate a **RMV:CCSLK** input message as previously described, and the use of the **UCL** (unconditional) option bypasses protective defensive checks.
- The 7xx (uninhibit) menu selection only affects a *locally inhibited* CCSLK (CCSLK must have an *L* in the **INH** column on the 1533 page).
- The 72xx (unblock) menu selection only affects a *locally blocked* CCSLK (CCSLK must have an *L* in the **BLK** column on the 1533 page).
- The 5xx (test) menu selection only affects an *active or inhibited* state (*L and/or R* in the **INH** column on the 1533 display page).
- In 5E13 and later software releases, it is possible to inhibit or allow periodic signal link tests (SLTs) via the **INH:CCS-PSLT** and **ALW:CCS-PSLT** commands, respectively. Periodic SLTs can be inhibited or allowed on a GSM, link set, or CCSLK basis.

Related command **OP:CCS-PSLT** allows craft personnel to obtain the inhibit or allow status for periodic SLTs on one or more CCSLKs.

- **RMV:MD** manually removes the intra-SM MD link on a specific GSM. This message has rare legitimate uses, because removal of the MD link terminates *all* CCS services on its GSM; an unconditional qualifier is required.

- `RST:MD` attempts the restoration of the intra-SM MD link on a specific GSM.
- `RMV:TRK` manually removes an SDL port (using a DEN identifier for DFI access, or a NEN for DNU-S access); an unconditional qualifier is required (unless the parent CCSLK is DACT).
- `RST:TRK` attempts the restoration of an SDL port (using a DEN identifier for DFI access, or a NEN for DNU-S access).
- Use traditional `RMV/RST:PSUPH` requests to reconfigure PH3 hardware, which is supporting a CCSLK/MD link. Sufficient protections exist to ensure that CCS operation is not severely affected, but unconditional options are available that usually override such protections:
 - Active PH3s supporting CCS functionality may not be switched manually.
 - When restoring a PH3, a CCS channel group may not be specified on the command line, if it is already assigned to an ACT PH.
 - PHs supporting CCS functionality cannot be manually removed, unless a standby spare PH3 exists on the same PSU shelf; when no spares are available, the unconditional option allows removal of a PH3 supporting CCS links, but fails if the intra-SM MD link is assigned.
- Use traditional requests `RMV/RST DFI, FAC, DSUSCD, TMUX, STEFAC, STSFAC, VT1FAC, or DS1SFAC` to reconfigure DFI/DNU-S hardware/facilities, which support an SDL port. Sufficient protections exist to ensure CCS operation is not adversely affected, but unconditional options are available that usually override such protections.
 - Associated DFI/DNU-S hardware/facilities may not be conditionally removed, unless all child SDLs or their parent CCSLKs are manually removed first; unconditional options override these protections.
 - If associated DFI/DNU-S hardware/facilities are restored, attempts are made to restore child SDL ports and their associated CCSLKs automatically.

NOTE: The definitions of DNU-S components change in the 5E13 software release. All references in provisioning and corrective maintenance procedures in Sections 13 and 14 clearly highlight the differences between pre-5E13 software releases and 5E13 and later software releases.

12.3 ENGINEERING

12.3.1 Hardware Resources

No new hardware is introduced for these features. The SS7-PSU platform is built using existing SM/SM-2000 hardware. See "PSU Hardware Platform," Section 12.1.2 .

Formal provisioning rules allow up to *four* CCS signaling links (CCSLKs) to be equipped on a PSU channel group, or three CCSLKs plus the intra-SM message delivery (MD) link. Recent change places no restrictions on the number of protocol handler version 3 (PH3) spares on a PSU shelf supporting CCS services. It places no restrictions on the organization of signaling data link (SDL) access facilities chosen.

While this provisioning freedom exists, there are engineering guidelines to assign resources such that local congestion can be avoided and that basic reliability criteria are considered.

The following high-level guidelines are valid for all typical GSMs. For atypically -engineered GSMs (either the number of ISUP trunks or TCAP users), detailed guidelines/formulas can be found in 235-070-100, *Administration and Engineering Guidelines*.

- At least *one spare PH3* should be provisioned on every packet switch unit (PSU) shelf that supports any CCS activity. If non-CCS PH3s exist on the same shelf, at least two spares should be provisioned, one for each software image type. There should be *at least two PH3 channel groups* containing CCSLKs, such that pairs (typical) of CCSLKs assigned to a given link set (LS) or combined link set (CLS) can be distributed across at least two PHs (for reliability). The intra-SM MD link should be assigned to a *separate channel group*.
- The previous configuration of PH3s is sufficient to support the ISUP trunk/TCAP traffic loads offered on any SM/SM-2000 GSM in the current release.

Additional alternate signaling routes may be defined to account for rare multiple failures or severe congestion conditions in intermediate signaling points (if desired). Also, direct CCSLKs to another end office may be defined to accommodate high volumes of interoffice traffic. These additional CCSLKs should be assigned to existing channel groups (up to a maximum of four CCSLKs per ST7 channel group), if possible, as total GSM signaling load is distributed over all the CCSLKs.

- The digital facility interface (DFI) or digital networking unit - SONET (DNU-S) access vehicle should be chosen for reliability. Mated pairs of CCSLKs (especially those to different regional STPs) should *not exit* the GSM on the *same* facility. Also, outside plant with embedded CCSLKs to the same adjacent point code (APC) should use diverse routes (if extra T1 spans are not required to accommodate this arrangement).

In 5E14 and later software releases, PH22 hardware is available for CCS signaling terminations, but reliability guidelines cited in this section are still valid.

12.3.2 Software Resources

This feature requires additional timeslots and uses memory for the new PH image required in the SM. In non-SM-2000s, additional memory is required to support the larger software configuration necessary for SS7 on a PSU platform provisioning.

12.3.3 Transition Considerations

For details, see "SS7 - PSU Feature Implementation," Section 13 .

12.4 RECENT CHANGE PROVISIONING

See 235-118-255 for 5E14, *Recent Change Reference* for detailed information on allowed values.

The service provider enables the MTP Node Restart procedure part of the SS7 PSU Whitebook MTP Enhancements feature by populating the following fields in RC/V view 8.22, SECURED FEATURE UPGRADE:

FIELD	VALUES
FEATURE ID	177
MODULE	OFC
PASSWD	(Obtain from Lucent Technologies SFID Administrator)
ACTIVE	Y

The following fields support the SS7 PSU Whitebook MTP Enhancements feature:

RC/V VIEW	VIEW NAME	FIELD	ALLOWED VALUES
16.1	GLOBAL SM	RESTART OPTION	NONE
		SUFFICIENT RTE	0 to 100
		SUFFICIENT LNK	0 to 100
16.2	LEVEL 3 TIMER PARAMETERS	ANSI TRA WAIT	30 to 60
		ANSI TRW WAIT	3 to 60
		ANSI TRA ANSWER	30 to 90
16.10	SIGNALING POINT CODE	RESTART OPTION	NONE or RESTART
		REMOTE INIT SSN ALW	Y or N
16.21	SCCP PARAMETER DEFINITION	REMOTE SCCP MGMT	Y or N
		LOCAL INIT SPEC	Y or N
		LOCAL INIT SSN ALW	Y or N

12.5 ADMINISTRATION

12.5.1 Measurements

Measurements of the operation or failure of the message transfer part (MTP) signaling links, signaling connection control part (SCCP), or MTP destination point codes (DPCs) were not provided for 5ESS®-2000 switch VCDX GSMs in the 5E11 software release. Also, message throughput measurements for CCS protocol handlers (PHs) or packet interface (PI) were not provided in the 5E11 software release.

MTP, SCCP, and DPC 30-minute traffic (TRFC30) measurements were introduced in the 5E12 software release; they provide data for CCS network traffic studies, and aid in provisioning of resources or services. Unlike most TRFC30 measurements, collection or printing control for these new measurements is provisioned using RC/V. (See "MTP/SCCP Measurements Provisioning," Section 13.4, for details.) Following is a high-level overview of these measurements:

- **TRFC30 Section 230, MTP SIGNALING LINK.** Specifies traffic characteristics, seconds of availability or unavailability, as well as a variety of congestion or failure conditions of a specific CCS signaling link (CCSLK).
- **TRFC30 Section 233, SIGNALING CONNECTION CONTROL PART.** Specifies the number of global title translations (GTTs) and numerous peg counts of failures for the SCCP capability on a specific GSM.
- **TRFC30 Section 234, MTP POINT CODE.** Specifies seconds of unavailability and link set access data for a specific destination point code (DPC) of a GSM.

These PH and PI measurements were modified in the 5E12 software release:

- **Section 51, PACKET INTERFACE MEASUREMENTS.** Specifies message throughput to or from the SMP, in addition to current overload or occupancy values for a specific SM's packet interface. This data on GSMs can be used to detect overengineering of combined CCS/ISDN services using the PI.
- **Section 52, CHANNEL GROUP MEASUREMENTS.** Specifies message throughput to or from the SMP, in addition to current overload or occupancy value for a specific protocol handler. This data on a PH supporting CCS services can be used to detect overengineering of specific CCS signaling links (CCSLKs).

Existing traffic measurements for supported ISDN user part (ISUP) and transaction capabilities application part (TCAP) services are available in the 5E11 and later software releases for GSM traffic on a VCDX. In the 5E12 software release, GSM contributions to the above measurements are provided, as are advanced services platform (ASP) measurements.

For details on the measurements mentioned in this section, refer to 235-070-100A1, *5ESS®-2000 Switch Traffic and Plant Measurements*.

12.5.2 Billing

This feature has no impact on billing.

12.5.3 Operation, Maintenance and Administration Part Routing Verification User's Guide

12.5.3.1 Introduction

This section is a user's guide for operation, maintenance and administration part (OMAP) routing verification tests, available for global SM (GSM) SS7 signaling platforms in the 5E13 and later software releases.

There are two types of OMAP route verification tests:

- Message transfer part (MTP) routing verification test (MRVT), described in Section 12.5.3.2 .
- Signaling connection control part (SCCP) routing verification test (SRVT), described in Section 12.5.3.3 .

The sections below discuss the implementation of MRVT/SRVT for GSM PSU signaling platforms, including the use of input/output messages unique to the 5ESS®-2000 switch.

12.5.3.2 MTP Routing Verification Tests

12.5.3.2.1 Overview of the MRVT Mechanism

The MTP routing verification test (MRVT) is intended to address the problems of administering the SS7 network from the perspective of MTP routing from a specific GSM. MRVT is a method of verifying the effectiveness of provisioned MTP routes, between the initiating signaling point (SP) and a specific terminating SP. In the context of the descriptions to follow, the initiating SP is always the origination point code (OPC) of a specific GSM. The terminating SP must be a destination point code (DPC) known to that GSM, as provisioned by the procedure "Define New Destination Point Codes," Section 13.1.7 . The SPs along an MTP route between the GSM OPC and a specific DPC are known as intermediate SPs, and are always signaling transfer points (STPs).

The actual routes used by MRVT correspond to the provisioned route sets for a particular DPC. The route sets can include ordinary link sets (LSs) or combined link sets (CLSs). From the perspective of MRVT, a CLS is considered to be two separate routes: each of the constituent LSs. Up to seven LSs may be provisioned as route candidates to a given DPC; a primary route and multiple alternate routes can be defined (including some CLSs).

While normal MTP routing attempts to use the primary route, if available, followed by alternate routes (in the order of provisioning) under failure conditions, MRVT treats all possible routes to a given DPC as equal candidates. The primary goal of the MRVT mechanism is to send test messages via every provisioned route to a DPC, and to receive acknowledgments for all test messages received by the DPC. This ensures that two-way MTP communication is possible between the GSM's OPC and a given DPC, regardless of the possible provisioned route actually used at any given time.

For such testing to be completely successful, these conditions are required:

- All SPs along a route between the GSM and a given DPC (including the DPC itself) must support MRVT functionality.
- MRVT verifies the accuracy and consistency of the *administrable* MTP routing data at each SP involved in transporting a signaling message between the GSM's OPC and a given DPC. Administrable routing data is static, and can be modified by an equivalent recent change mechanism (for the GSM, the 16.10 recent change view is used).

MRVT is not intended to check *dynamic* routing characteristics, which define the route in effect at a given time. Dynamic routing data is determined not only by static data, but also SP processor outages, link failures, and recovery within the network. Dynamic states, however, can impact the success or failure of MRVT if certain routes between SPs are inaccessible or there are actual processor outages.

To illustrate possible routing paths, consider Figure 12.5-1 .

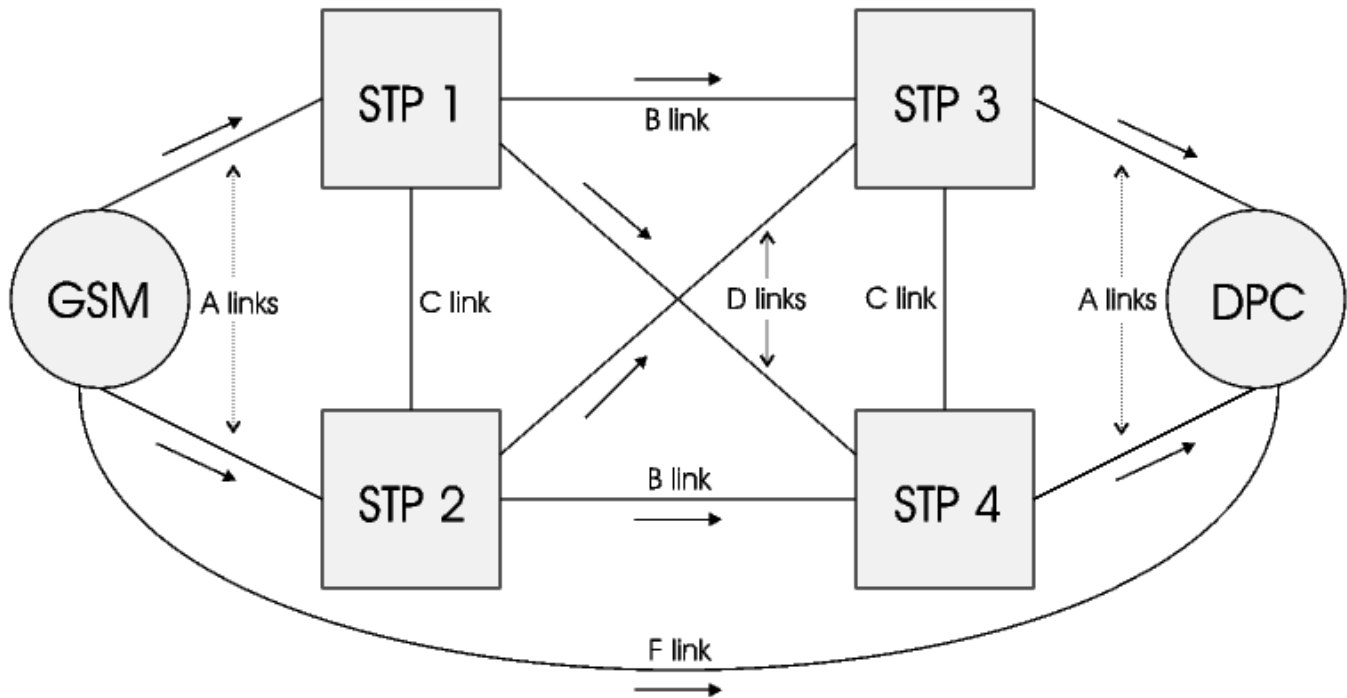


Figure 12.5-1 Typical SP Routing Paths

In Figure 12.5-1, STP 1/STP 2 and STP 3/STP 4 represent regional/local mated STP pairs. The GSM has a direct F-link path to the target DPC, as well as a typical CLS to a mated STP pair via A-links. The arrows illustrate possible intermediate paths used to route an MTP message between SPs as the message is sent from the GSM to the target DPC. The actual composite path used for a particular MTP message depends on primary/alternate route provisioning at every SP, and the dynamic availability of particular link sets or the SPs themselves. C-links between mated STP pairs can be used to route messages in certain fault conditions, but they are excluded from MTP routing verification testing (and corresponding route possibilities are not shown in Figure 12.5-1).

MRVT use three types of OMAP message (which is actually a TCAP client, using SCCP transport):

- (1) The MTP routing verification test (MRVT) message initiates the test of administrable MTP routing data at any SP that receives it. The MRVT message contains:
 - The point code of the initiator of the test (i.e., the OPC of the GSM).
 - The point code of the terminator of the test (i.e., the target DPC).
 - The maximum value of intermediate STPs that may be crossed before an MRVT message reaches the target DPC (the default value is 2, but craft personnel can alter this value, as described in Section 12.5.3.2.2).
 - A trace request flag, which indicates whether a trace list of crossed STPs is to be sent from the terminating DPC to the originating GSM (this is a craft personnel option discussed in Section 12.5.3.2.2).
 - The trace list of STPs crossed thus far, prior to sending a specific MRVT message to the next SP.

To avoid confusion, when used by itself, MRVT refers to the entire test mechanism, while actual messages are denoted as MRVT messages.

- (2) The MTP routing verification acknowledgment (MRVA) message acknowledges each MRVT message received, and it encodes a summary of partial test results received from other SPs.
- (3) The MTP routing verification result (MRVR) message conveys a list of STPs crossed in a test from the target DPC directly back to the initiating GSM (if requested by craft personnel). It is also used as a general mechanism to report errors detected at any SP receiving an MRVT message. The details of MRVR contents are described in Section 12.5.3.2.3.

In MTP routing verification testing, all SPs on a valid route between the initiating GSM and the terminating DPC actively participate in the test. These MRVT messages are spawned:

- The initiating GSM sends MRVT messages to *all* adjacent point codes (APCs) for a provisioned route to a target DPC (the terminator of the MRVT session).

Provisioned routes include *all* primary/alternate link sets (LSs) for the target DPC defined in ODD. If a provisioned route is a combined link set (CLS), MRVT considers *both* constituent LS routes. If multiple link sets are provisioned to access the *same* APC, *any one* of those LSs is used to access the APC.

- An APC receiving an MRVT message from the GSM checks its own static routing data, and sends MRVT messages to *each* of its adjacent SPs that correspond to valid routes that can forward an MTP message to the final terminating DPC.
- Each additional intermediate STP that receives an MRVT message, in turn, sends MRVT messages on all valid MTP routes that can forward a message to the terminating DPC.
- When the terminating DPC receives an MRVT, no further MRVT messages are sent, and the acknowledgment process begins (described below).

Figure 12.5-2 illustrates the MRVT message flow on the CCS network shown in Figure 12.5-1.

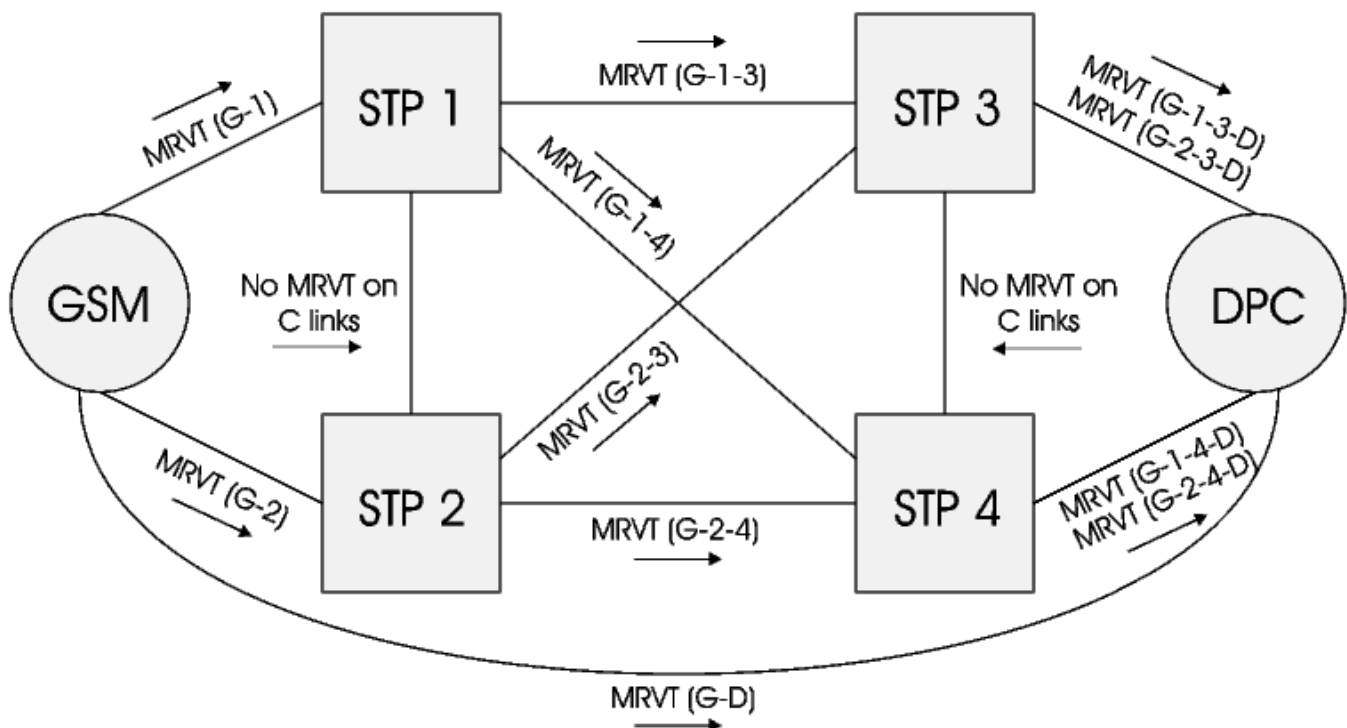
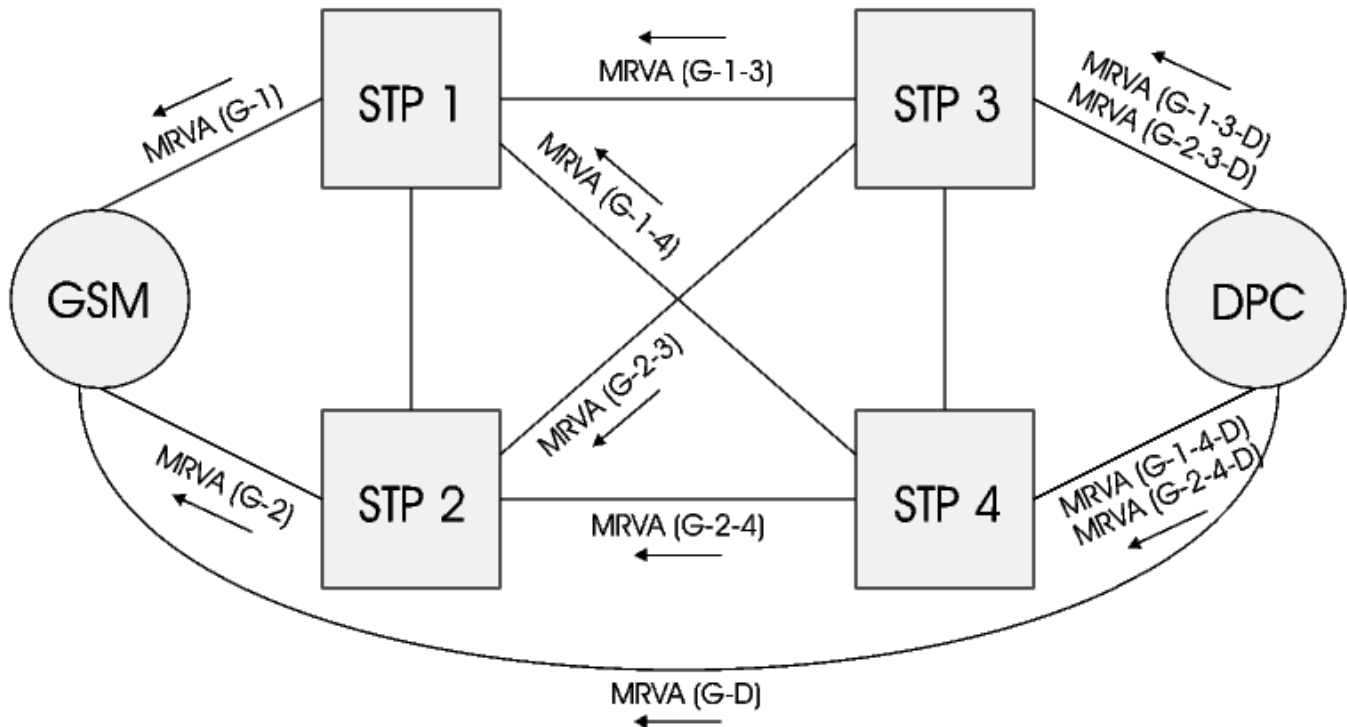


Figure 12.5-2 Typical MRVT Message Flow

The alphanumeric sequence enclosed in parentheses for each MRVT message shows the network path as the testing progresses. The first letter "G" represents the GSM that initiates the MRVT session, and the last entry specifies the intermediate STP number ("D" for the terminating DPC) that receives the specific MRVT message. This sequence (excluding the initiating GSM and terminating DPC) at the DPC provides identification of all STPs crossed for a particular path, and is known as a *trace list*.

When MRVT messages arrive at the terminating DPC, the acknowledgment process begins. The MRVA messages sent are shown in Figure 12.5-3.

**Figure 12.5-3 Typical MRVA Message Flow**

The following fault-free scenario describes the acknowledgment sequence:

- The target DPC realizes it is the "test terminator" and does not attempt to propagate further MRVT messages; the MRVT messages received specify the DPC as the terminator.
- The DPC sends MRVA messages back to the originator of every MRVT message received. In this fault-free scenario, MRVA (G-1-3-D), MRVA (G-2-3-D), MRVA (G-1-4-D), and MRVA (G-2-4-D) all indicate "success" and are returned to the adjacent STP that sent the corresponding MRVT message. To provide a sorting capability at the recipient, the TCAP transaction identifier from the MRVT message is returned in the MRVA message.
- At an intermediate STP, handling of MRVA messages is more complicated in many cases.

At an intermediate SP, the *receipt* of each MRVT message may cause the *generation* of one or more MRVT messages to adjacent SPs downstream toward the DPC. Before the STP can send an acknowledgment to the originator of the *received* MRVT message, it must first receive MRVA messages from downstream SPs to which MRVT messages were sent.

For example, consider STP 1 on Figure 12.5-2. When STP 1 receives the MRVT (G-1) message from the GSM, it spawns downstream MRVT (G-1-3) and MRVT (G-1-4) messages. Referring to Figure 12.5-3, a fault-free scenario requires that MRVA (G-1-3) *and* MRVA (G-1-4) messages are received from STP 3 and STP 4, respectively, *before* the MRVA (G-1) message is sent back to the GSM.

- Similarly, three MRVT messages are spawned at the GSM as a result of the craft personnel request to investigate the target DPC: MRVT (G-1), MRVT (G-2) and MRVT (G-D) messages in Figure 12.5-2. Before craft personnel receive the test results, the fault-free scenario requires that *all* three MRVA messages be received first: MRVA (G-1), MRVA (G-2), and MRVA (G-D), as shown in Figure 12.5-3.

The above example is a very simplistic fault-free scenario. If the MRVT messages generated result in "successful" MRVA messages being returned in every case, the craft personnel initiating the test on the GSM are notified that all the routes provisioned for a DPC are "in fine working order." Thus far, error cases have not been considered, and finding routing errors is a primary purpose of the MRVT mechanism. In fact, MRVT should be initiated when routing faults are possible or likely:

- (1) Whenever a new DPC is provisioned (see the procedure "Define New Destination Point Codes," Section 13.1.7).
- (2) Whenever one or more routes to a DPC are changed (see the procedure "Modify Link Sets Serving a DPC," Section 13.1.13).
- (3) Whenever it is suspected that a route to an existing DPC is experiencing trouble, determined by a correlation of switch data such as machine detected interoffice irregularities (MDIIs) or poor call completion rates to a specific DPC.

In these error cases, craft personnel are provided with useful information about administrable routing errors on the local GSM, intermediate STP, or specified DPC. These errors are passed back to the initiating GSM by embedded failure data in MRVA messages, and more importantly by MRVR messages. Such cases are discussed in detail in other subsections.

The remaining MRVT subsections are decomposed as follows:

- Section 12.5.3.2.2 contains a description of the EXC:CCS-MRVT input message, with emphasis on choosing appropriate input parameters to cause the desired MRVT execution.
- Section 12.5.3.2.3 contains a description of the EXC CCS-MRVT and REPT CCS-MRVR output messages, noting the types of messages produced in successful and failed MRVT scenarios, and discussing error codes in more detail than the 235-600-750, *5ESS®-2000 Switch Output Message Manual*.
- Section 12.5.3.2.4 provides examples of various successful MRVT scenarios, including input/output message contents, as well as the OMAP message flows between signaling points.
- Section 12.5.3.2.5 provides examples of various types of MRVT failures, illustrating input/output message contents, as well as the OMAP message flow between SPs.

12.5.3.2.2 MRVT Input Message Formats

In the 5ESS®-2000 switch, MTP routing verification testing is initiated on GSM PSU signaling platforms (in 5E13 and later software releases) via the EXC:CCS-MRVT command.

The simplest format is:

EXC:CCS,MRVT,DPC=a,OPC=b

where *a* is the 9-digit DPC of interest, and *b* is the 9-digit OPC of the GSM of interest (to obtain a complete list of GSMs in the office and their corresponding OPCs, issue the `OP:CCS,GSM` command). This format initiates an MRVT session with one restriction: the number of *STPs crossed* in any MRVT path is *not greater than 2* (the count includes STPs and does not include the initiating GSM or terminating DPC).

If craft personnel want to specify a different maximum number of STPs that can be crossed, the input should be modified as follows:

EXC:CCS,MRVT,DPC=a,OPC=b,STPS=c

where *c* is the maximum number (in the range 1-15) of STPs that can be crossed by any path.

To request a *trace list of intermediate STPs crossed* for all possible MRVT streams that successfully reach the DPC, either of the above formats may be modified as follows:

EXC:CCS,MRVT,DPC=a,OPC=b,TRACE

EXC:CCS,MRVT,DPC=a,OPC=b,STPS=c,TRACE

If successful, the trace for each traversed path is sent by the DPC via an `MRVR` message directly to the GSM.

An MRVT request may not start because of local conditions in the originating office/GSM, such as:

- a duplicate request exists (the same OPC/DPC combination is already under test),
- the OPC specified does not correspond to any GSM in the office,
- the OPC or DPC is specified in an invalid format,
- the specified GSM is isolated or initializing,
- the specified DPC is inaccessible or not provisioned for the target GSM,
- the loss of the intra-SM MD link causes all CCS operations on the GSM to cease, or
- the maximum number of MRVTs for the specified GSM is already running (see "Operation, Maintenance and Administration Part Provisioning," Procedure 13.1.22, to update the number of simultaneous MRVTs possible).

See the 235-600-700, *5ESS®-2000 Switch Input Message Manual* and the 235-600-750, *5ESS®-2000 Switch Output Message Manual* for more details and exact outputs produced in these types of failure cases.

12.5.3.2.3 MRVT Output Message Formats

There are four types of MRVT output messages possible in fault-free scenarios.

The first output message produced indicates that the MRVT session has *started*:

EXC CCS MRVT DPC=a OPC=b TEST STARTED

MAX STPS ALLOWED TO CROSS: c

TRACE REQUESTED

where *a* is the 9-digit DPC, *b* is the 9-digit OPC of the GSM, and *c* is the maximum number of STPs that can be crossed during testing (the number entered on the input command, or the default value of 2). `TRACE REQUESTED` indicates that craft personnel requested a *trace* of STPs crossed (the string `NO TRACE REQUESTED` is output if no

trace is requested).

The next group of output messages provides the results of each MRVA returned to the GSM (in response to each MRVT message sent), assuming "complete success."

```
EXC CCS MRVT DPC=a OPC=b SUCCESS
MRVA RECEIVED FROM: d
MRVA RESULT: SUCCESS
```

where *d* is the 9-digit adjacent point code (APC) returning the MRVA message to the GSM. The SUCCESS qualifier on the first line refers to the results of the entire test; the result in the *third* line refers to the individual MRVA reported.

Another type of output message is possible if a TRACE option is included in the input command:

```
EXC CCS MRVT DPC=a OPC=b SUCCESS
TRACE MRVR FROM: a
NUMBER OF STPS CROSSED: e
TRACE LIST:
f . . . . .
```

The MRVR messages with the trace list are always sent from terminating DPC *a*, and one MRVR is returned for each MTP path traversed in the test. The output message contains the number *e* of intermediate STPs crossed, and the supplemental information provided is the actual trace list *f*, which may identify 0 to 15 9-digit point codes (possibly in multiline format). The trace list excludes the initiating GSM's OPC and the terminating DPC.

The last output message received, after all MRVA reports and optional MRVR traces are produced, is:

```
EXC CCS MRVT DPC=a OPC=b TEST ENDED
```

Departing from the above fault-free scenario, a wide variety of failures or partial success conditions can occur.

The output messages reporting MRVA results have this more flexible form in partial success/failure cases:

```
EXC CCS MRVT DPC=a OPC=b g
MRVA RECEIVED FROM: d
MRVA RESULT: h
ERROR DETECTED:
i
```

where *g* is the summary result for the entire MRVT session spawned by the GSM (values selected from PARTIAL SUCCESS or FAILURE, under the assumption of a faulty scenario), and *h* is the result returned by a particular MRVA, selected from SUCCESS, PARTIAL SUCCESS, or FAILURE (for faulty scenarios, at least one MRVA must be classified as PARTIAL SUCCESS or FAILURE).

If an MRVA result is PARTIAL SUCCESS or FAILURE, one or more error conditions *i* are listed, on multiple lines if necessary (the line ERROR CODES: is omitted and *i* is blank if the MRVA result is SUCCESS).

The MRVT error codes are listed in Table 12.5-1 .

Table 12.5-1 MRVT Error Codes

Error Code	Description
LOOP	A loop is detected if an adjacent SP to which an MRVT message would normally be sent already exists in the trace list received. The MRVT message received by an intermediate STP always contains a trace of previous STPs traversed.

	A similar failure occurs if an attempt is made by an intermediate STP to send an MRVT back to the initiating GSM's OPC.
EXCESSIVE LENGTH ROUTE	The number of intermediate STPs in the <i>trace list</i> in a received MRVT message equals the <i>maximum number of STPs allowed to be crossed</i> encoded in the message, and the receiver is <i>not</i> the terminating DPC. This maximum STP crossed parameter is <i>defaulted</i> to 2 unless the input command on the GSM specifies another value (any value in the range 1-15 is permitted).
UNKNOWN DESTINATION	The terminating DPC is not recognized in the MTP routing data at an intermediate STP.
INACCESSIBLE ROUTE	An MRVT message cannot be sent on a particular route from the initiating GSM or an intermediate STP. This means that the SCCP message (which encapsulates the MRVT message) cannot be transported due to an inaccessible or congested route (the link set to be used has no active CCSLs, the far-end SP prohibits the use of the link set, or local/remote congestion levels are too high to allow transport of test messages).
LOCAL CONDITIONS	If an intermediate STP cannot continue the test because of local conditions (that cannot be classified as an INACCESSIBLE ROUTE), an MRVA message is sent back to the originator of the MRVT message with this error (if possible). This failure is highly dependent upon the STP hardware architecture, and may include inability to access routing data, local overload conditions, or exceeding the maximum number of MRVT messages that can be handled at the STP. This error is not valid for the terminating DPC, because the DPC is not attempting to propagate MRVT messages; it can return or not return the MRVA message. The initiating GSM does not return MRVA messages to another SP, and this condition is not applicable.
UNKNOWN INITIATING POINT CODE	An intermediate STP or the terminating DPC has no knowledge of the initiating GSM's OPC in its MTP routing tables. Routing ability should be bidirectional. If the GSM's OPC is not a valid route at a given STP/DPC, it is impossible for that STP/DPC to send an error MRVR to the initiating GSM. Instead, an MRVA is returned to the originator of the MRVT message, with the UNKNOWN INITIATING POINT CODE error and an indication that no MRVR was sent; the SP receiving this MRVA sends an MRVR message to the initiating GSM, citing pertinent data associated with this error (if the GSM receives such an MRVA, it self-generates an equivalent MRVR).
TIMER EXPIRED	All expected MRVAs are not received within a prescribed time-out interval (T1 timer). For the initiating GSM, the timer is defined as $T1=D \times (N+1)$, where N is the number of STPs that can be crossed, as specified in the input message (or N=2 , the default), and D is the delay or expected processing/transmission time for MRVT/MRVA message exchange (this is recent changeable, as described in the procedure "Operation, Maintenance and Administration Part Provisioning," Section 13.1.22). On intermediate STPs, the time allotted is different, reduced by the number of STPs already crossed, and affected by locally defined delay times.
WRONG SP	The MRVT message arrives at a signaling point that does not have STP functionality. This is not a valid error for the terminating DPC.
UNKNOWN ERROR CODE x	Failure codes x above the value of 8 are considered unknown by the GSM.

If the GSM cannot send an MRVT, a special output format is spawned internally by the GSM:

```

EXC CCS MRVT DPC=a OPC=b g
MRVT NOT SENT
ERROR DETECTED: INACCESSIBLE APC
POINT CODES AFFECTED:
j .....
```

where j represents the point codes that are inaccessible/congested (possible multiline format).

Another error type, `NETWORK ERROR`, could be specified in the above format; this corresponds to the inability of the SCCP to transmit the `MRVT` message to an APC.

For the case in which no `MRVA` is received due to the `TIMER EXPIRED` condition, another type of message is generated internally by the GSM:

```
EXC CCS MRVT DPC=a OPC=b g
MRVA NOT RECEIVED
ERROR DETECTED: TIMER EXPIRED
POINT CODES AFFECTED:
k .....
```

where k represents the point codes that did not return an `MRVA` in the time allotted (possible multiline format).

When an intermediate STP receives an `MRVT` message, it normally generates one or more `MRVT` messages itself on locally known routes used to forward MTP messages toward the terminating DPC. Before an `MRVA` message can be returned to the originator of the `MRVT` message received, the STP must receive all `MRVA` messages corresponding to `MRVT` messages sent (or the T1 guard timer at the STP expires).

Consider Figure 12.5-4 .

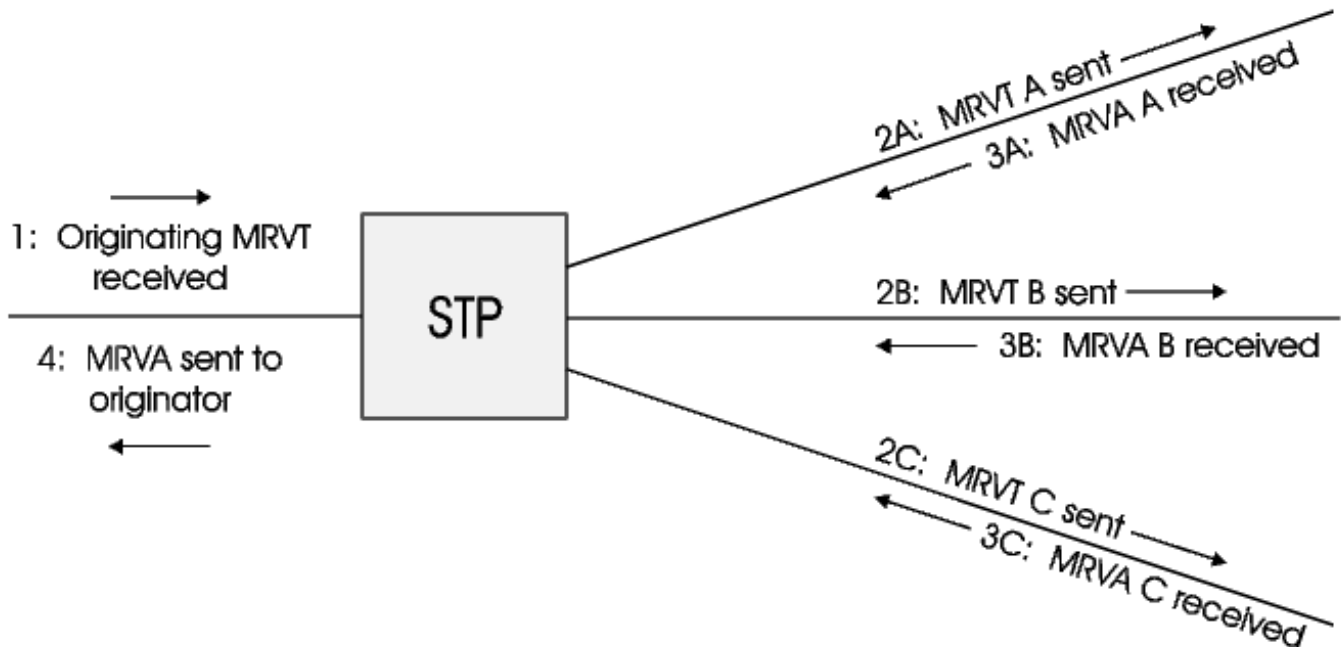


Figure 12.5-4 MRVT / MRVA Message Flow at an STP

Increasing time is represented by the sequence 1, (2A, 2B, 2C), (3A, 3B, 3C), 4. If the guard timer expires before all expected `MRVA` messages are received, missing `MRVAs` are considered to be received with a `FAILURE` result and a `TIMER EXPIRED` error code. `MRVAs` received after the timer expires are discarded.

Each of the `MRVA` messages 3A, 3B, 3C received also has a result/possible error code:

- If the result is `SUCCESS`, all downstream `MRVA` messages (on all valid routes between the STP and the terminating DPC) have a `SUCCESS` result.

- If the result is `PARTIAL SUCCESS`, at least one downstream `MRVA` message has a `SUCCESS` result, and at least one has a `FAILURE` result.

Also included is a composite error code, which is a "logical ORing" of all types of errors reported by downstream `FAILURE MRVA` messages (as described in Table 12.5-1).

- If the result is `FAILURE`, then all downstream `MRVA` messages have `FAILURE` results. The composite error code is also included.

The flow of `MRVA` processing starts at the terminating `DPC` (where only `SUCCESS` or `FAILURE` results are possible) and passes through intermediate `STPs` until `MRVA` messages are delivered to the initiating `GSM`. For the `STP` example in Figure 12.5-4 , the results/error codes from `MRVAs` for events 3A, 3B, 3C are "logically combined," using the above algorithm, to produce the `MRVA` message in event 4. If the testing process is halted at an intermediate `STP` (and the terminating `DPC` is never reached), the `MRVA` backward flow starts at that `STP`.

The `MRVA` messages received by the `GSM` represent the quality of a *particular route* emanating from that `GSM`. Any error codes returned are for one or more paths used to reach the terminating `DPC`. `MRVA` message data provides no information about the source (`STP` or `DPC`) of those errors; `MRVA` responses contain only summary error information.

The assumption is that one or more signaling points are experiencing problems. Because `MRVAs` do not contain the `SP` where the error occurred or supplemental information necessary to isolate the problem, more data must be provided to the `5ESS`®-2000 switch craft personnel. This additional troubleshooting information is provided by the `MTP` routing verification result (`MRVR`) message.

One type of `MRVR` message is output when craft personnel request that a trace list be returned (see Section 12.5.3.2.3). This type of supplemental information (i.e., a successful trace) may still be delivered in error conditions, provided `MRVT` messages reach the terminating `DPC`, and that `DPC` is capable of returning the trace to the `GSM`. The only difference is that the overall test result `SUCCESS` on the first line of output is replaced by `PARTIAL SUCCESS`.

The more interesting case of detailed error location is supplied by the output message:

```
EXC CCS MRVT DPC=a OPC=b g
MRVR RECEIVED FROM: m
ERROR DETECTED: n
SUPPLEMENTAL INFO:
p .....
```

where `g` is the *overall test result* `PARTIAL SUCCESS` or `FAILURE`, `m` is the signaling point where the error is detected (which could be the initiating `GSM` or terminating `DPC`), `n` is the error type (listed in Table 12.5-1), and `p` is optional supplemental information, as listed in Table 12.5-2 . *Administrative* actions that should be taken in response to `MRVRs` received at the `GSM` are also included in Table 12.5-2 entries.

Such `MRVR` messages are delivered directly from the `SP` detecting the error to the initiating `GSM` via the preferred `MTP` route (rather than the interdependent `MRVT/MRVA` message chain). There is one exception for the `UNKNOWN INITIATING POINT CODE` case, which is described in the appropriate Table 12.5-2 entry.

In addition to `MRVRs` sent, the `STP/DPC` returns a `PARTIAL SUCCESS` or `FAILURE MRVA` message that contains the error codes for failures detected to the originator of the `MRVT`. Also, `STPs` that detect an error *usually* cease propagating any other downstream `MRVT` messages (there are exceptions, as noted in Table 12.5-2).

Table 12.5-2 Supplemental `MRVR` Error Information

Error Code	Supplemental Information/Administrative Actions
LOOP	For the detected loop, the STP that would route an <i>MRVT</i> message to an adjacent point code already in the trace list is identified as the <i>m</i> parameter in the <i>MRVR</i>, and the list of STPs involved in this detected routing loop is provided as supplemental information <i>p</i> (this is the trace list in the received <i>MRVT</i> message, plus the receiving STP, plus the duplicated point code specified in the reporting STP's routing data). The detected routing loop must be corrected. The administrators of responsible STPs identified in the <i>MRVR</i> must be contacted. Primary candidates are the STP returning the <i>MRVR</i>, and the STP identified as the duplicate signaling point that would create the loop.
EXCESSIVE LENGTH ROUTE	If an <i>MRVT</i> message is received by a point code other than the terminating DPC, <i>and</i> the number of STPs in the trace list equals the maximum number of STPs that can be crossed (this data is provided in the received <i>MRVT</i> message: defined by craft personnel in the range 1-15, or the default value of 2), an excessive length route is detected. The <i>MRVR</i> parameter <i>m</i> is the STP detecting the excessive route length, and <i>p</i> contains the trace list. If a longer route cannot be tolerated, the GSM administrator can choose a new one. If a longer route can be tolerated, re-execute the <i>MRVT</i> command, but increase the <i>STPS</i> parameter and specify the <i>TRACE</i> option. If the route of interest is longer but viable, no further action need be taken (this is usually the case when the default value of 2 STPs crossed was used in the original test).
UNKNOWN DESTINATION	In this case, an intermediate STP does not recognize the terminating DPC in its MTP routing tables. The STP detecting this problem is identified as <i>MRVR</i> parameter <i>m</i> (no other information is provided). This is a very severe problem. Either the affected route must be deleted or replaced on the GSM (see the procedure "Modify Link Sets Serving a DPC," Section 13.1.13), or the administrator of the STP reporting the error must be contacted to correct routing data.
INACCESSIBLE ROUTE	When attempting to send an <i>MRVT</i> message (from an intermediate STP), it is determined that an identified route is inaccessible or congested, and an <i>MRVR</i> is generated. The <i>MRVR</i> parameter <i>m</i> is the point code detecting the inaccessibility problem, and <i>p</i> is a list of one or more downstream point codes that are inaccessible/congested. In addition to the <i>MRVR</i>, the SP detecting the error returns an <i>MRVA</i> with the INACCESSIBLE ROUTE error code to the <i>MRVT</i> originator, but further downstream <i>MRVT</i> processing ceases on the <i>affected routes only</i>. If the GSM detects such an error, error message equivalents are generated internally. An inaccessible route is a <i>dynamic</i> problem, and the <i>MRVT</i> outcome is inconclusive. Re-execute the same <i>MRVT</i> command later when the affected route is presumably accessible.
LOCAL CONDITIONS	If an intermediate STP cannot process a received <i>MRVT</i> message because of local problems at that STP, an <i>MRVR</i> is generated. The <i>MRVR</i> parameter <i>m</i> is the STP with the local problem (this is duplicated as supplemental information <i>p</i>). This assumes that the STP is sane enough to send the <i>MRVR</i>. The <i>MRVT</i> outcome is inconclusive because a particular STP or the terminating DPC has a <i>dynamic</i> local problem. Re-execute the same <i>MRVT</i> command later, as the problem must be assumed to be transient.
UNKNOWN INITIATING POINT CODE	If an intermediate STP or the terminating DPC has no knowledge of the initiating

	GSM's OPC in its MTP routing table, an MRVR should be generated, but there is no way to send it back to the GSM. Instead, all further downstream MRVT processing ceases (if applicable), and a FAILURE MRVA with the UNKNOWN INITIATING POINT CODE error is sent to the MRVT originator. This MRVA has a special indication that <i>no MRVR was sent</i>. Upon receipt of such an MRVA, the <i>receiving STP</i> actually sends the MRVR to the GSM, with MRVR parameter <i>m</i> being the point code actually generating the MRVR and <i>p</i> being the point code that has no knowledge of the initiating GSM. The administrator of the SP without knowledge of the GSM's OPC (not the SP sending the MRVR) must be notified to establish a bidirectional route in static data.
TIMER EXPIRED	One or more expected MRVAs are not received before the T1 guard timer (described in Table 12.5-1) expires. The detecting intermediate STP sends an MRVR to the GSM, with parameter <i>m</i> being the STP detecting the expired timer, and supplemental information <i>p</i> containing a list of actual point codes that do not return the MRVR. If the GSM detects the expired timer, an equivalent error message is internally generated. An intermediate STP detecting the time-out sends an MRVA with TIMER EXPIRED error to the MRVT originator. This returned MRVA can contain other error codes because some expected MRVAs at that signaling point may be received in time. Should the missing MRVAs that triggered the timer expiration be received later, they are discarded by the receiving STP/GSM. The MRVT outcome of the affected route is inconclusive, and should be retried later. It can be assumed that real-time problems at the affected STP delayed the MRVA response, or a problem occurs after receiving the MRVT message for processing. Another possibility is that the STP/DPC that fails to respond with an MRVA may not support OMAP functionality. Contact the administrator of that STP/DPC.
WRONG SP	If an MRVT message is sent to a signaling point that is not the terminating DPC or does not have STP functionality, an MRVR is generated. The parameter <i>m</i> is the SP detecting the problem, and supplemental information <i>p</i> contains the trace list of crossed STPs, noting that the last STP on the list has routed the message to the wrong SP. This is a serious problem. The <i>last</i> STP in the MRVR trace list has sent an MTP message to a signaling end point (SEP) that does not provide STP functionality. The administrator of the STP <i>sending</i> the MRVT message is required to correct MTP routing tables.
UNKNOWN ERROR CODE x	If an STP/DPC (non-Lucent Technologies® product) detects an error that is not recognized by the GSM, an MRVR is sent to the GSM anyway. When reported, the parameter <i>m</i> is the STP/DPC reporting the error, and <i>k</i> is UNKNOWN ERROR CODE <i>x</i>, where <i>x</i> is the actual code, greater than 8 (supplemental information <i>p</i> also indicates the PC reporting the error). Contact the administrator of the STP/DPC returning the MRVR message with this error code to determine whether the reported problem is valid or not.

When an intermediate STP or terminating DPC receives an MRVT message, the processing of MRVRs/MRVAs proceeds with this sequence:

- (1) If the receiving STP/DPC cannot process the *MRVT* any further because of local conditions (see Table 12.5-1 entry), *MRVR/MRVA* messages are immediately generated with the LOCAL CONDITIONS error code, and further *MRVT* processing ceases.
- (2) If the test can proceed, it is verified that the initiating GSM's OPC is known. If the OPC is *not* known, then an *MRVA* message is immediately generated with the UNKNOWN INITIATING POINT CODE error code, and further *MRVT* processing ceases. This is not possible at an APC associated with the GSM.
- (3) If the initiating GSM's OPC is known, it is determined if the SP receiving the *MRVT* possesses STP functionality. If the SP does *not* have STP functionality, then *MRVR/MRVA* messages are immediately generated with the WRONG SP error code, and further *MRVT* processing ceases.

This is not a valid check at the terminating DPC.

- (4) If the initiating GSM's OPC is known and STP functionality is available at an intermediate STP, it is determined if MTP routing has knowledge of the terminating DPC. If MTP routing does *not* have knowledge of the terminating DPC, then *MRVR/MRVA* messages are immediately generated with the UNKNOWN DESTINATION error code, and further processing of that *MRVT* message ceases.

This is not a valid check at the terminating DPC.

- (5) If an intermediate STP passes the above checks, it produces a list of possible routes to the tested DPC, and these additional checks are made:
 - If a *routing loop* (see Table 12.5-1) is detected, then *MRVR/MRVA* messages are immediately generated with the LOOP error code, and further processing of that *MRVT* message ceases.
 - If no routing loops are detected, a check for *excessive length route* is made (see Table 12.5-1). If an excessive length route is detected, then *MRVR/MRVA* messages are immediately generated with the EXCESSIVE LENGTH ROUTE error code, and further processing of that *MRVT* message ceases.
 - If no routing loop/excessive length errors are detected, static routing data is polled to determine possible routes to the terminating DPC. Dynamic routing data is consulted to determine if the selected routes are inaccessible or congested. If *any* inaccessible or congested route is found, an *MRVR* with the INACCESSIBLE ROUTE error code is generated, and further *MRVT* processing on *that route only* ceases. Errors reported in *MRVA* messages are a composite of these inaccessible routes, as well as the results of any *MRVT* messages successfully sent on accessible routes.

These are not valid checks at the terminating DPC.

- (6) In the absence of any of the above error conditions, an intermediate STP spawns *MRVT* messages on all available downstream routes to the terminating DPC. A T1 guard timer (see Table 12.5-1) is set to monitor *MRVA* responses. If the timer expires, an *MRVR* message with the TIMER EXPIRED error code is sent for *all* *MRVAs* not received (if any fail to arrive). An *MRVA* is sent back to the *MRVT* originator with a PARTIAL SUCCESS or FAILURE result, including the TIMER EXPIRED error code.

Such a timer is also set in the GSM, and an internally generated error message is produced.

An intermediate STP or terminating DPC always sends *MRVR* messages *first*, via the preferred MTP route to the initiating GSM. Additionally, T1 guard timers are based on the slow process of converging *MRVAs*, and all *MRVRs* should arrive before that timer expires.

MRVAs arriving after the T1 guard timer expires are discarded, but this is *not* the case if an *MRVR* arrives late *and* it is

reporting an error (craft personnel requested trace MRVRS are discarded). Instead, a message of this form is produced by the GSM:

```
REPT CCS MRVR DPC=a OPC=b
MRVR RECEIVED FROM: m
ERROR DETECTED: n
SUPPLEMENTAL INFO:
p .....
```

where the parameters listed are as described for MRVRS arriving on time. If the UNKNOWN DESTINATION error (parameter n) is present, the message is accompanied by a MINOR alarm.

12.5.3.2.4 Successful MRVT Scenarios

For Example 1 of a successful MRVT session, consider the network architecture shown in Figure 12.5-5.

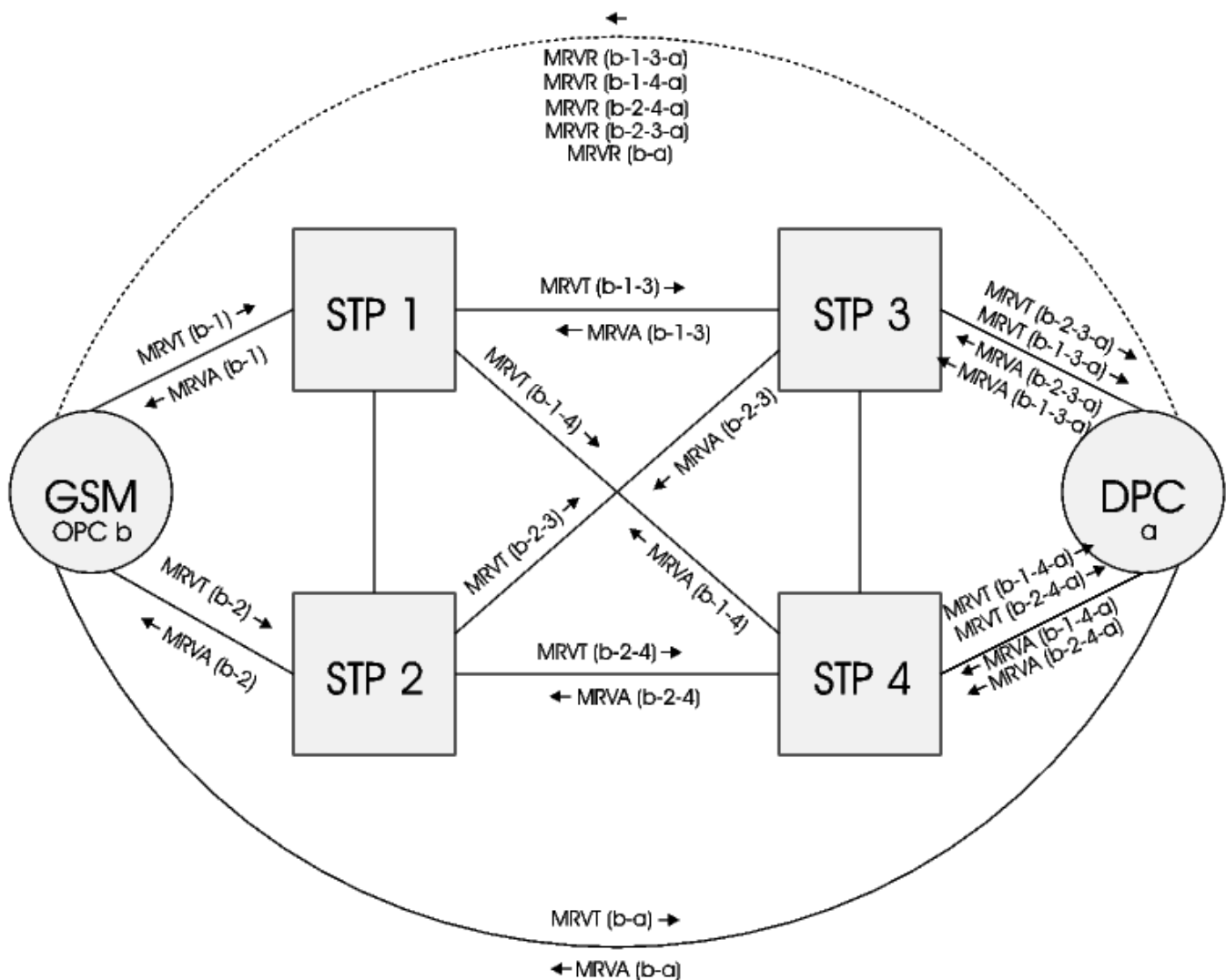


Figure 12.5-5 MRVT Example 1

In Example 1, craft personnel issue this command on the 5ESS®-2000 switch containing the target GSM:

EXC:CCS,MRVT,DPC=a,OPC=b,TRACE

where a is the 9-digit DPC of interest, and b is the 9-digit OPC of the GSM of interest.

In the message flows illustrated in Figure 12.5-5, a and b represent the DPC and OPC, respectively; 1, 2, 3, and 4 represent the signaling points STP 1, STP 2, STP 3, and STP 4, respectively. The MRVT/MRVA message flows are described in Section 12.5.3.2.1. The five MRVR messages are a result of the TRACE option; the dashed path indicates that MRVRs are returned via the primary MTP route from the DPC to the GSM.

The sequence of output messages produced on the 5ESS®-2000 switch follows, where the variables a, b, sp1, sp2, sp3, and sp4 represent *9-digit point codes* of the DPC, OPC, STP 1, STP 2, STP 3, and STP 4, respectively (similar variables are used in all examples).

EXC CCS MRVT DPC=a OPC=b TEST STARTED
MAX STPS ALLOWED TO CROSS: 2
TRACE REQUESTED

EXC CCS MRVT DPC=a OPC=b SUCCESS
MRVA RECEIVED FROM: sp1
MRVA RESULT: SUCCESS

EXC CCS MRVT DPC=a OPC=b SUCCESS
MRVA RECEIVED FROM: sp2
MRVA RESULT: SUCCESS

EXC CCS MRVT DPC=a OPC=b SUCCESS
TRACE MRVR FROM: a
NUMBER OF STPS CROSSED: 2
TRACE LIST:
sp1 sp3

EXC CCS MRVT DPC=a OPC=b SUCCESS
TRACE MRVR FROM: a
NUMBER OF STPS CROSSED: 2
TRACE LIST:
sp1 sp4

EXC CCS MRVT DPC=a OPC=b SUCCESS
TRACE MRVR FROM: a
NUMBER OF STPS CROSSED: 2
TRACE LIST:
sp2 sp3

EXC CCS MRVT DPC=a OPC=b SUCCESS
TRACE MRVR FROM: a
NUMBER OF STPS CROSSED: 2
TRACE LIST:
sp2 sp4

EXC CCS MRVT DPC=a OPC=b SUCCESS
TRACE MRVR FROM a
NUMBER OF STPS CROSSED: 0

EXC CCS MRVT DPC=a OPC=b TEST ENDED

For Example 2 of a successful MRVT session, consider the provisioned routes illustrated in Figure 12.5-6 .

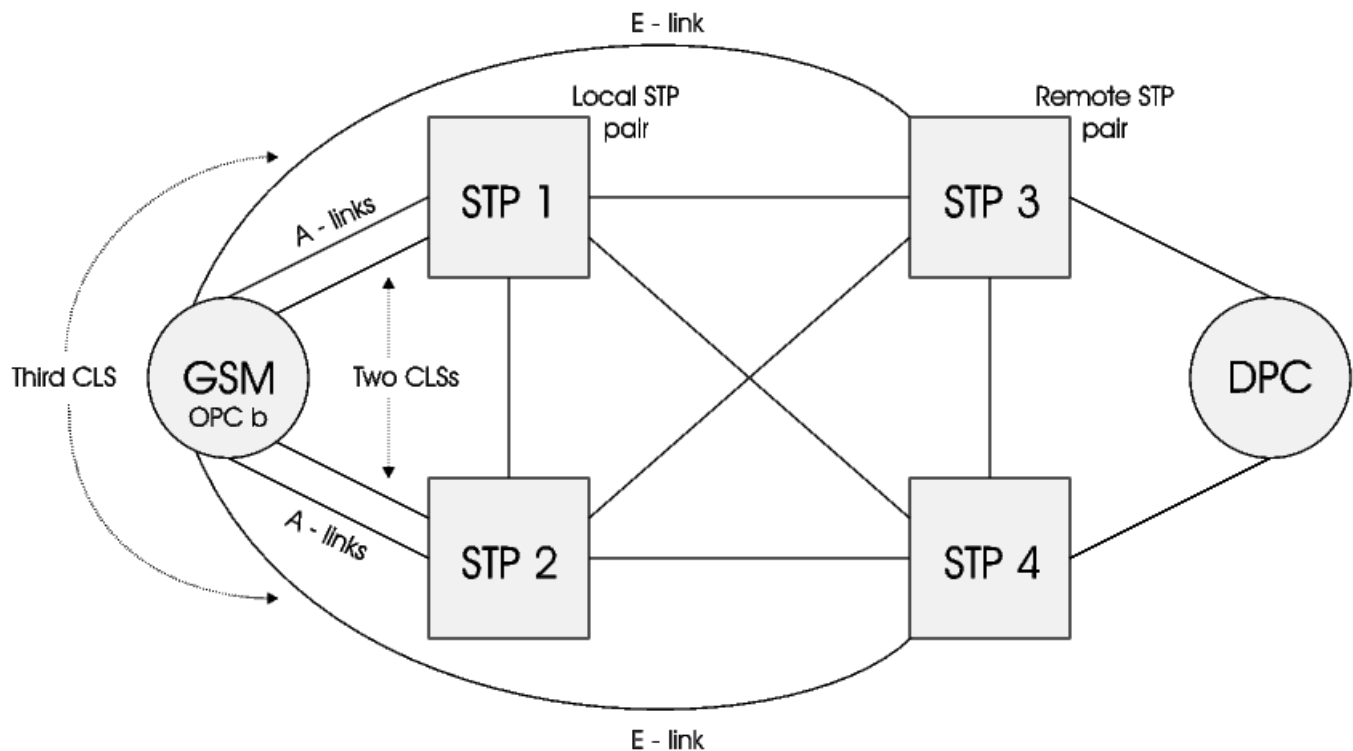


Figure 12.5-6 MRVT Example 2 Routes

In this case, provisioned routing to the specified DPC is:

- A *NORMAL* (primary A-link) combined link set (CLS) route to a local STP pair (STP 1, STP 2)
- An *ALTERNATE* (backup A-link) route to the same STP 1/STP 2 pair, using a *different* CLS
- An *ALTERNATE* (backup E-link) CLS route to a remote STP pair (STP 3/STP 4)

The interesting point here is that it is possible to provision a GSM with *different* link sets as backup routes to the *same* adjacent point code (APC), such as STP 1 and STP 2 in this example; this is not possible with CNI or many other vendors' switches. From the perspective of MTP routing verification testing, however, the *pair* of link set routes to the same APC are treated as a *single MRVT route*; it should be noted that MTP access to the APC via *either* link set is verified by the MTP level 3 signaling link test mechanism, so either LS can be used in MTP routing verification testing without affecting results.

The MRVT/MRVA message flow for MRVT Example 2, spawned by the basic MRVT command

EXC:CCS,MRVT,DPC=a,OPC=b

is illustrated in Figure 12.5-7 .

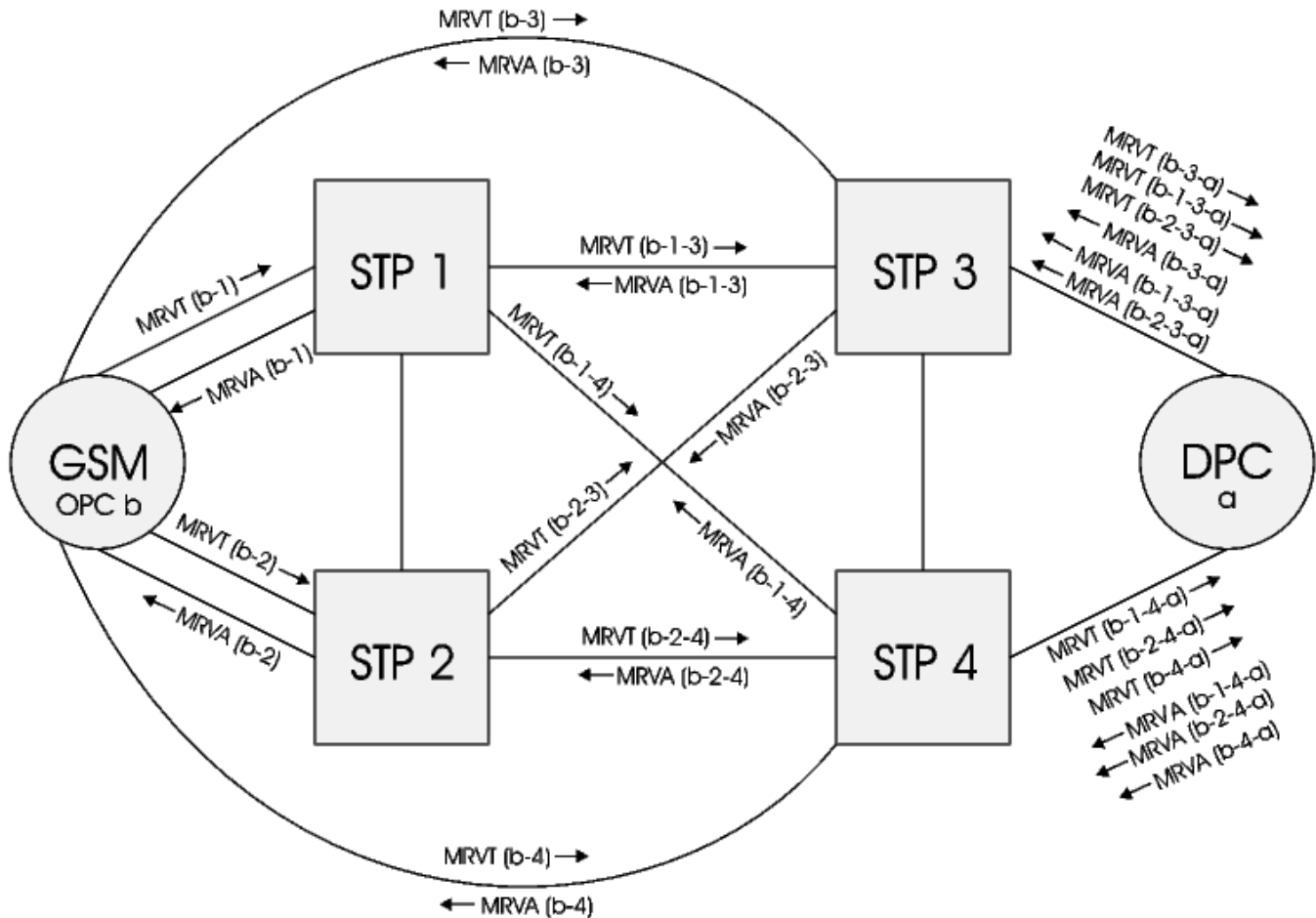


Figure 12.5-7 MRVT Example 2 Message Flow

The output messages produced at the GSM for this test are:

```
EXC CCS MRVT DPC=a OPC=b TEST STARTED
MAX STPS ALLOWED TO CROSS: 2
NO TRACE REQUESTED
```

```
EXC CCS MRVT DPC=a OPC=b SUCCESS
MRVA RECEIVED FROM: sp1
MRVA RESULT: SUCCESS
```

```
EXC CCS MRVT DPC=a OPC=b SUCCESS
MRVA RECEIVED FROM: sp2
MRVA RESULT: SUCCESS
```

```
EXC CCS MRVT DPC=a OPC=b SUCCESS
MRVA RECEIVED FROM: sp3
MRVA RESULT: SUCCESS
```

```
EXC CCS MRVT DPC=a OPC=b SUCCESS
MRVA RECEIVED FROM: sp4
MRVA RESULT: SUCCESS
```

EXC CCS MRVT DPC=a OPC=b TEST ENDED

12.5.3.2.5 Partial Success or Failure MRVT Scenarios

This section describes MRVT scenarios in which one or more routing faults are detected during testing (these are the more interesting cases).

For MRVT Example 3, consider the network architecture between a GSM and a specified DPC shown in Figure 12.5-8 .

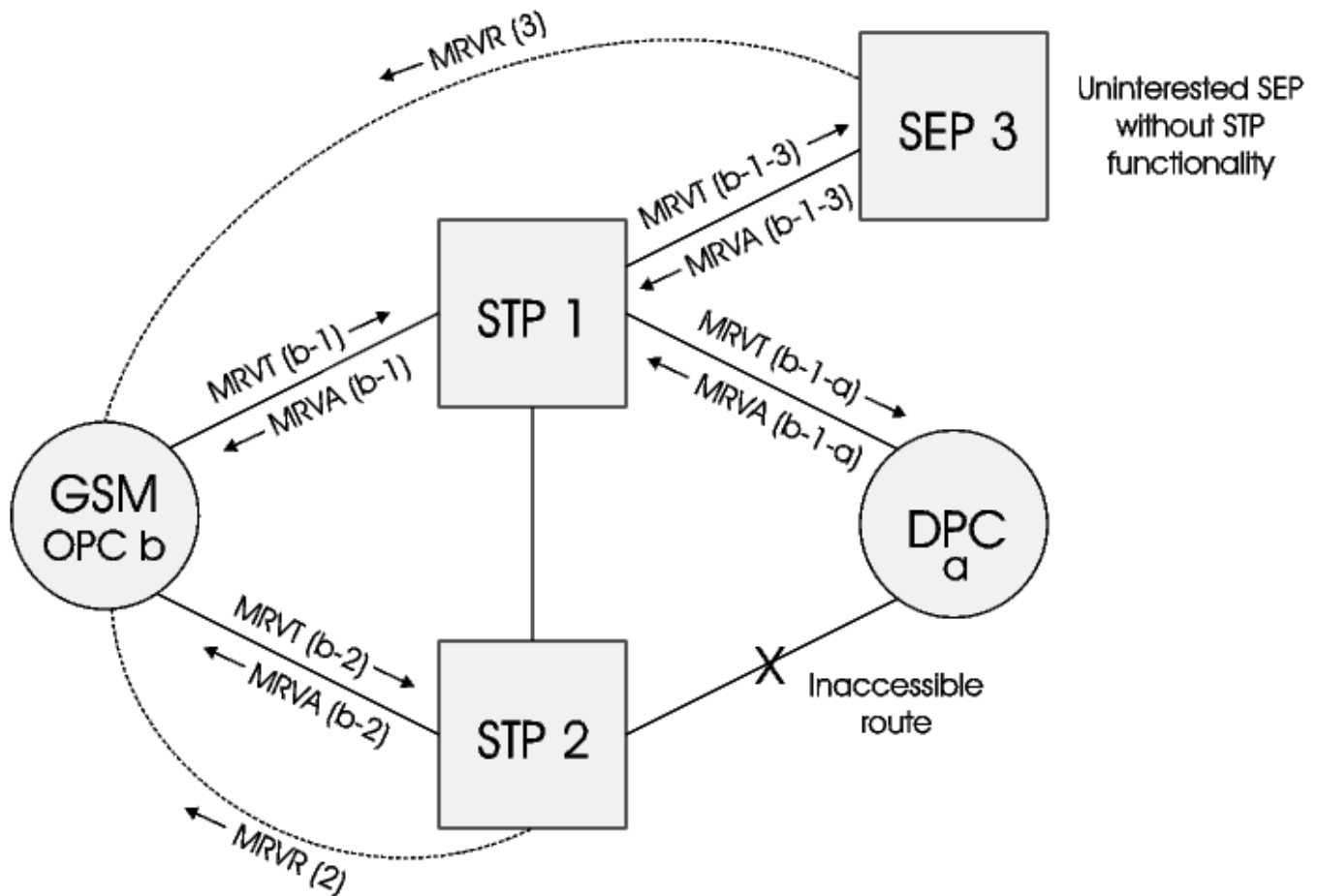


Figure 12.5-8 MRVT Example 3 Message Flow

In Figure 12.5-8 , there are two problems that MRVT should detect:

- STP 1 has incorrect routing data that indicates SEP 3 (a signaling endpoint office with no STP functionality) is a valid route to the target DPC (in addition to the valid direct route to the DPC), and
- the route between STP 2 and the target DPC is inaccessible.

If the default MRVT session is spawned by the input command

EXC:CCS,MRVT,DPC=a,OPC=b

then this output sequence is expected:

EXC CCS MRVT DPC=a OPC=b TEST STARTED
MAX STPS ALLOWED TO CROSS: 2
NO TRACE REQUESTED

EXC CCS MRVT DPC=a OPC=b PARTIAL SUCCESS
MRVA RECEIVED FROM: sp1
MRVA RESULT: PARTIAL SUCCESS
ERROR DETECTED:
WRONG SP

EXC CCS MRVT DPC=a OPC=b PARTIAL SUCCESS
MRVA RECEIVED FROM: sp2
MRVA RESULT: FAILURE
ERROR DETECTED:
INACCESSIBLE ROUTE

EXC CCS MRVT DPC=a OPC=b PARTIAL SUCCESS
MRVR RECEIVED FROM: sp2
ERROR DETECTED: INACCESSIBLE ROUTE
SUPPLEMENTAL INFO:
a

EXC CCS MRVT DPC=a OPC=b PARTIAL SUCCESS
MRVR RECEIVED FROM: sp3
ERROR DETECTED: WRONG SP
SUPPLEMENTAL INFO:
sp1

EXC CCS MRVT DPC=a OPC=b TEST ENDED

The first MRVR report indicates sp2 (STP 2) detected an inaccessible route, and supplemental information specifies the inaccessible point code a (the DPC). The second MRVR report indicates the point code sp3 (the unrelated SEP) received an MTP message to be forwarded to another destination, but sp3 does not possess STP functionality; the supplemental information is a *trace list* of SPs that lead to this erroneous route (in this case, the single point code sp1). There is no explicit information about the one successful route (b-sp1-a) provided because a TRACE option was not requested. The only hint that at least one route was successful is overall test result of PARTIAL SUCCESS.

For MRVT Example 4, consider the network architecture shown in Figure 12.5-9 .

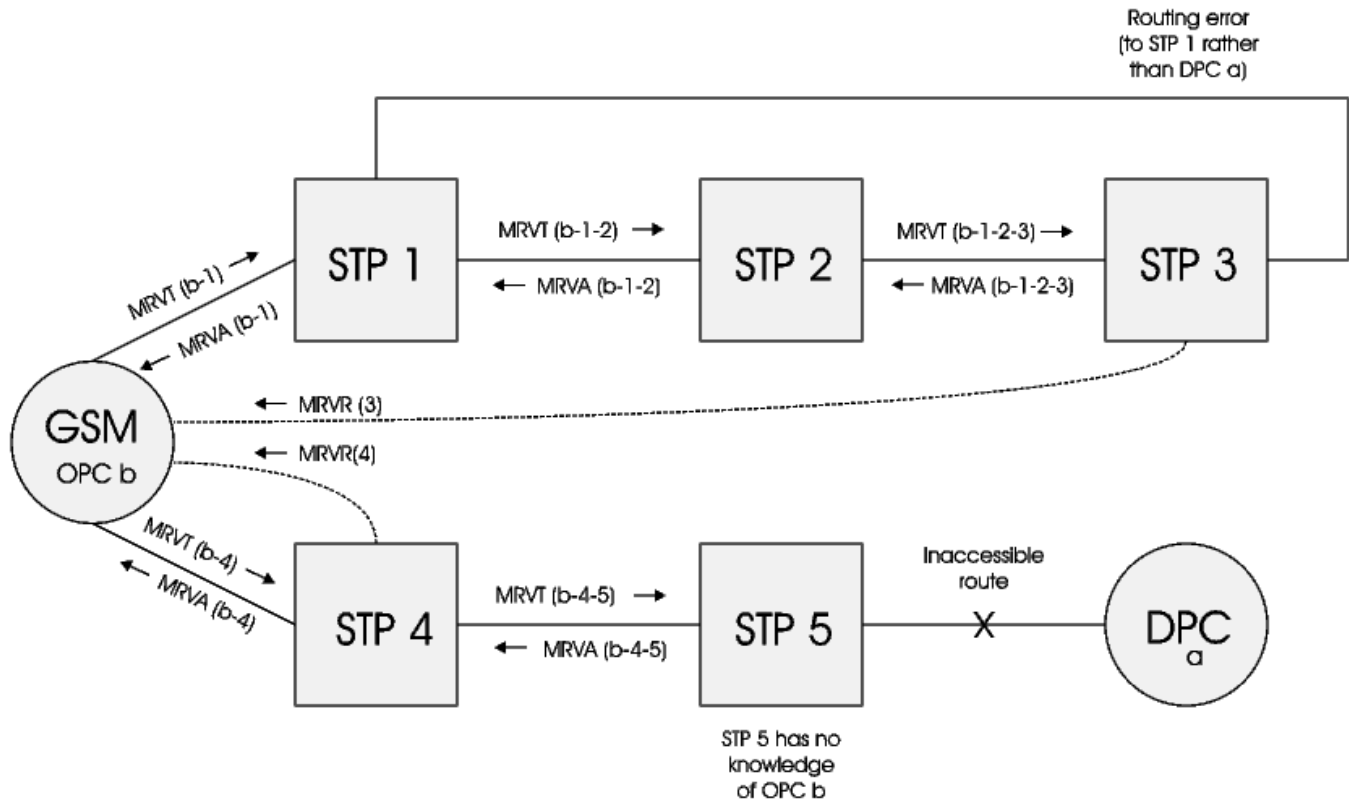


Figure 12.5-9 MRVT Example 4 Message Flow

Several problems exist in this example. STP 3 has a static routing data error, which would direct the message back to STP1 (rather than to the DPC), which would create a *routing loop*. Also, STP 5 has multiple problems: it has no *backward* routing knowledge of the initiating GSM's OPC, and the route to the target DPC is inaccessible anyway.

The basic MRVT input command

```
EXC:CCS,MRVT,DPC=a,OPC=b
```

produces these output messages:

```
EXC CCS MRVT DPC=a OPC=b TEST STARTED
MAX STPS ALLOWED TO CROSS: 2
NO TRACE REQUESTED
```

```
EXC CCS MRVT DPC=a OPC=b FAILURE
MRVA RECEIVED FROM: sp1
MRVA RESULT: FAILURE
ERROR DETECTED:
LOOP
```

```
EXC CCS MRVT DPC=a OPC=b FAILURE
MRVA RECEIVED FROM: sp4
MRVA RESULT: FAILURE
ERROR DETECTED:
UNKNOWN INITIATING POINT CODE
```

```
EXC CCS MRVT DPC=a OPC=b FAILURE
```

MRVR RECEIVED FROM: sp3

ERROR DETECTED: LOOP

SUPPLEMENTAL INFO:

sp1 sp2 sp3 sp1

EXC CCS MRVT DPC=a OPC=b FAILURE

MRVR RECEIVED FROM: sp4

ERROR DETECTED: UNKNOWN INITIATING POINT CODE

SUPPLEMENTAL INFO:

sp5

EXC CCS MRVT DPC=a OPC=b TEST ENDED

The supplemental information in the first MRVR report shows the potential LOOP, if STP 3 (point code sp3) would send an MRVT message to STP 1 (duplicated point code sp1), which was already crossed.

In the second MRVR sent from STP 4, STP 5 is identified as the signaling point that cannot route back to the GSM (identified in supplemental information sp5); STP 4 is performing a service that is impossible for STP 5 to accomplish, based upon information returned in MRVA (b-4-5). The inaccessible route between STP 5 and the DPC is not reported because the ability to route back to the initiating GSM is verified first.

For MRVT Example 5, consider the network architecture in Figure 12.5-10. There are several problems: STP 2 is unable to process MRVTs further due to local conditions (but can respond with an MRVA), and there is an inaccessible route from STP 5 to the DPC. Additionally, the MRVA sent from the DPC to STP 3 is delayed internally (does not arrive at STP 3 until after the guard timer expires).

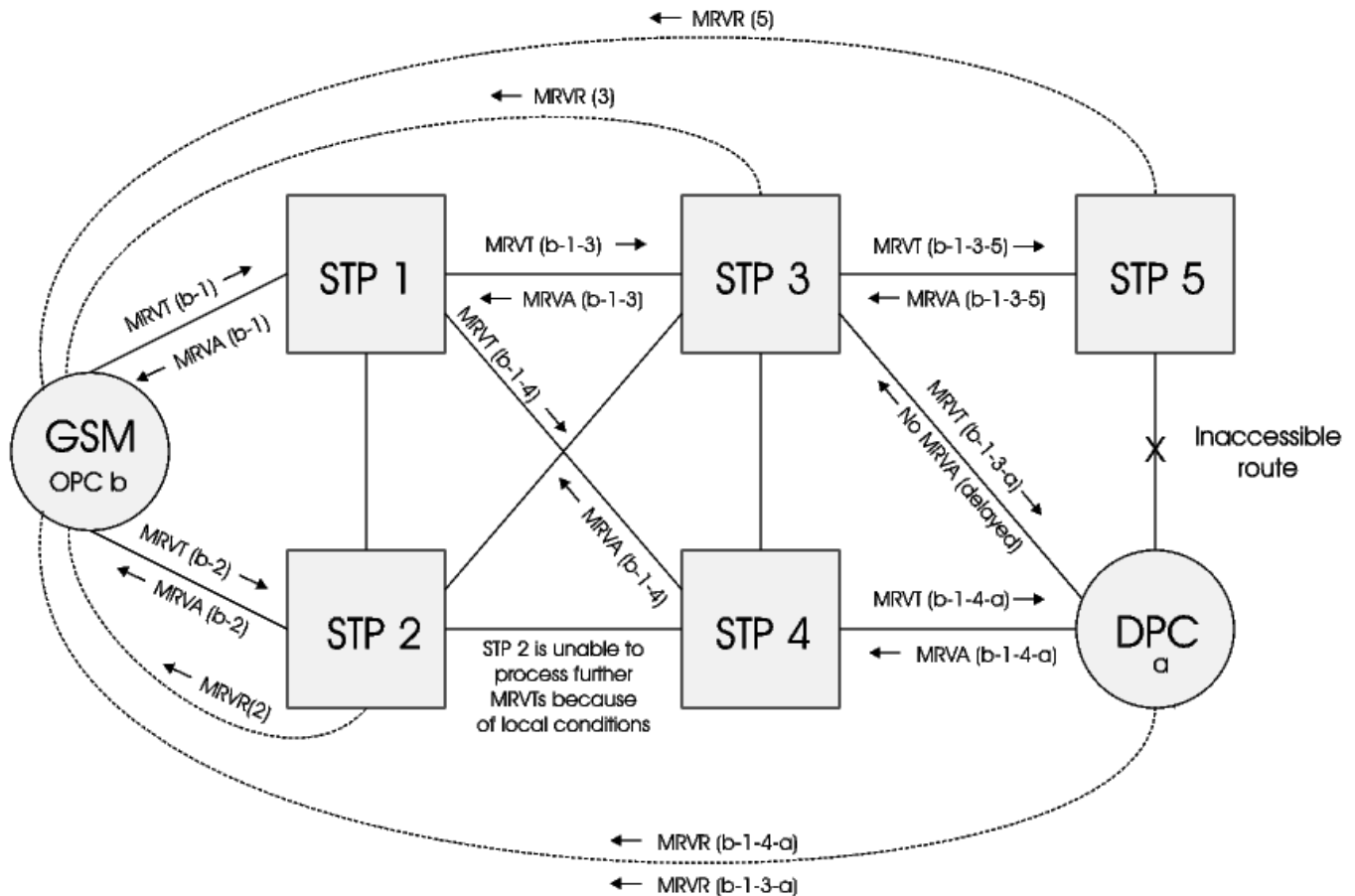


Figure 12.5-10 MRVT Example 5

In this example, a *trace list* is requested with the input command:

EXC: CCS, MRVT, DPC=a, OPC=b, TRACE

The complex output messages expected for this example are:

```
EXC CCS MRVT DPC=a OPC=b TEST STARTED
MAX STPS ALLOWED TO CROSS: 2
TRACE REQUESTED
```

```

EXC CCS MRVT DPC=a OPC=b PARTIAL FAILURE
MRVA RECEIVED FROM: sp1
MRVA RESULT: PARTIAL SUCCESS
ERROR DETECTED:
INACCESSIBLE ROUTE
TIMER EXPIRED

```

```
EXC CCS MRVT DPC=a OPC=b PARTIAL SUCCESS
MRVA RECEIVED FROM: sp2
MRVA RESULT: FAILURE
ERROR DETECTED:
LOCAL CONDITIONS
```



```
EXC CCS MRVT DPC=a OPC=b PARTIAL SUCCESS
TRACE MRVR FROM: a
NUMBER OF STPS CROSSED: 2
TRACE LIST:
sp1 sp3
```

```
EXC CCS MRVT DPC=a OPC=b PARTIAL SUCCESS
TRACE MRVR FROM: a
NUMBER OF STPS CROSSED: 2
TRACE LIST:
sp1 sp4
```

```
EXC CCS MRVT DPC=a OPC=b PARTIAL SUCCESS
MRVR RECEIVED FROM: sp2
ERROR DETECTED: LOCAL CONDITIONS
```

```
EXC CCS MRVT DPC=a OPC=b PARTIAL SUCCESS
MRVR RECEIVED FROM: sp3
ERROR DETECTED: TIMER EXPIRED
SUPPLEMENTAL INFO:
a
```

```
EXC CCS MRVT DPC=a OPC=b PARTIAL SUCCESS
MRVR RECEIVED FROM: sp5
ERROR DETECTED: INACCESSIBLE ROUTE
SUPPLEMENTAL INFO:
a
```

```
EXC CCS MRVT DPC=a OPC=b TEST ENDED
```

Although the MRVA from STP 1 specifies two error codes, it is the MRVRs from STP 3 and STP 5 that segregate these errors and provide information to identify the source of each problem. The trace list (for point codes `sp1` and `sp3` crossed) is produced in the first output trace MRVR report, even though the MRVA from the DPC to STP 3 was delayed beyond the guard timer expiration (these are independent events).

For MRVT Example 6, consider the network configuration in Figure 12.5-11 . STP 3 is assumed to be able to route to the DPC, but has no provisioned MTP data to do so.

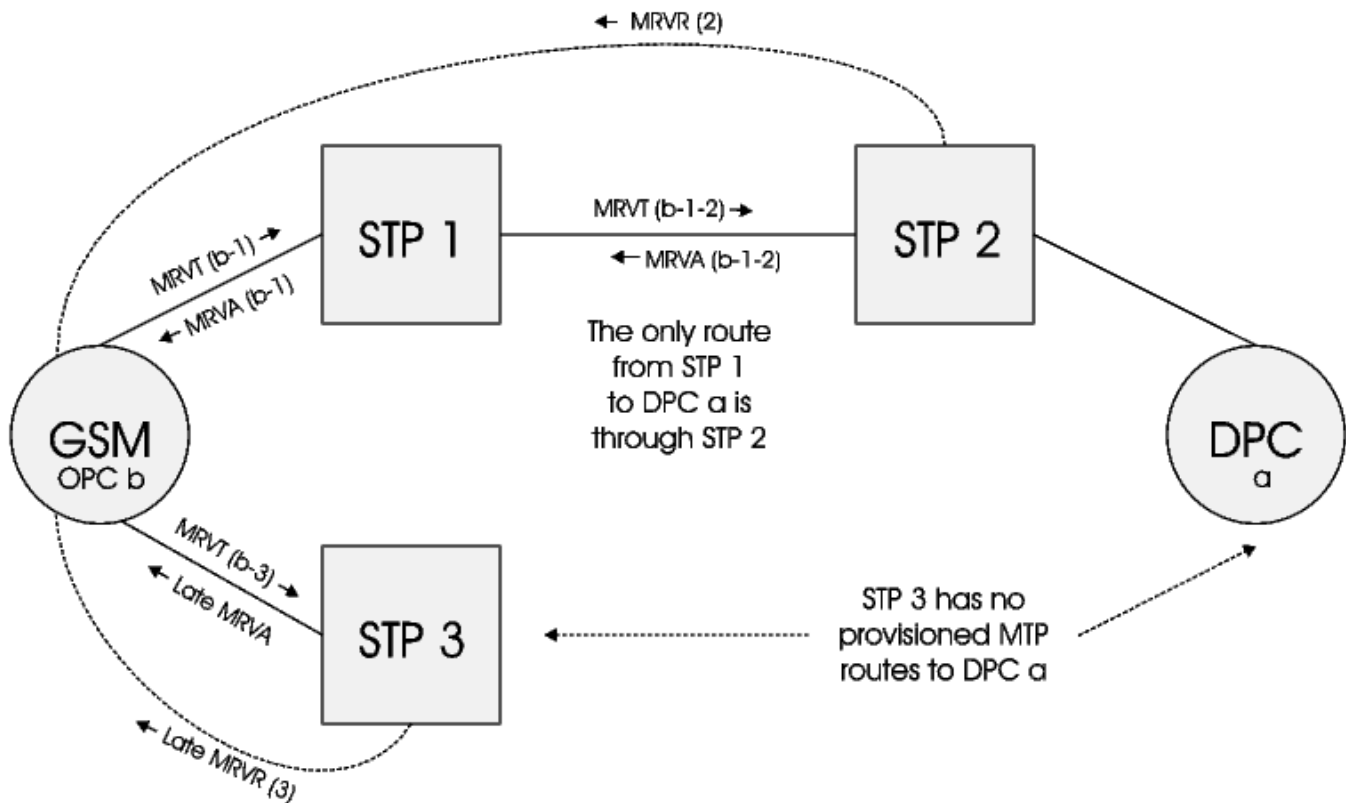


Figure 12.5-11 MRVT Example 6

For this example, the input command specifies that any route reaching the DPC must traverse at most one STP:

EXC:CCS,MRVT,DPC=a,DPC=b,STPS=1

These output messages are expected:

```
EXC CCS MRVT DPC=a OPC=b TEST STARTED
MAX STPS ALLOWED TO CROSS: 1
NO TRACE REQUESTED
```

```

EXC CCS MRVT DPC=a OPC=b FAILURE
MRVA RECEIVED FROM: sp1
MRVA RESULT: FAILURE
ERROR DETECTED:
EXCESSIVE LENGTH ROUTE

```

```

EXC CCS MRVT DPC=a OPC=b FAILURE
MRVA NOT RECEIVED
ERROR DETECTED: TIMER EXPIRED
POINT CODES AFFECTED:
spl

```

```

EXC CCS MRVT DPC=a OPC=b FAILURE
MRVR RECEIVED FROM: sp2
ERROR DETECTED: EXCESSIVE LENGTH ROUTE
SUPPLEMENTAL INFO:

```

sp1

```
EXC CCS MRVT DPC=a OPC=b TEST ENDED
```

```
* REPT CCS MRVR DPC=a OPC=b
```

```
MRVR RECEIVED FROM: sp3
```

```
ERROR DETECTED: UNKNOWN DESTINATION
```

```
SUPPLEMENTAL INFO:
```

```
a
```

The first MRVR reported from point code sp2 indicates that the maximum number of STPs allowed to be crossed (as specified by STPS in the input command) has been reached, and STP 2 is not the final destination. The trace list (in this case, only sp1) is included as supplemental information.

The second "MRVA not received" report is self-generated in the GSM when the T1 guard timer expires. The MRVA message arriving from STP1 *later* is discarded. The REPT CCS-MRVR message is still reported even though an MRVR message arrives late and the corresponding MRVT session is no longer active, *if* the message reports an error. The message has a MINOR alarm because of the UNKNOWN DESTINATION error type is reported.

12.5.3.3 SCCP Routing Verification Tests

12.5.3.3.1 Overview of SRVT

The signaling connection control part (SCCP) routing verification test (SRVT) mechanism tests SCCP global title translation (GTT) data for accuracy, completeness, and consistency in the SS7 network, and sectionalizes any routing problems discovered.

A global title (GT) is part of the called party address (it contains the type of service to be provided, as well as the digit string of the called number). It requires special processing at another office, network control point (NCP) or service control point (SCP) before the call can be completed. The intent of GTT and SCCP is to forward the GT to its ultimate destination for processing. This ultimate (or final) destination is a specific SCCP subsystem on a specific point code. When the final destination receives the message, including the GT, it sends a response to the initiator, which may provide instructions and/or the "real" called party address required to complete the call.

With this brief overview, several more detailed definitions (with emphasis on the GSM implementation) are required to understand the SRVT mechanism:

- The *translation type* (TT) is the part of the global title that refers to a particular Transaction Capability Application Part (TCAP) service such as NS800, LASS, or ISVM services.

The TT is a number from 0-255. To correlate the TT to a particular TCAP application, issue the command

```
OP:OFR, FORM=5537, DEVICE=xxx
```

where xxx is the medium to which the office records are directed (see the OP-OFR page in the 235-600-700, 5ESS®-2000 Switch Input Message Manual for more details). The output of the DIRECT SIGNALING APPLICATION form provides a list of all provisioned TCAP applications in the office, and their corresponding translation type. To verify that a particular application is supported on a specific GSM, at a recent change terminal, enter 8.42r to review the CCS TCAP APPLICATION view.

- The *digits* associated with a global title are the called party address (e.g., the NPA NXX XXXX code).
- A *global title translation* (GTT) is a mapping of one or more digits in the called party address for a particular TT to an SCCP route destination, which provides the required GT processing or a further GTT (used to forward the message closer to its ultimate destination). An SP that provides some level of GTT processing is known as a

transaction signaling point (TSP).

If a TSP has knowledge of the destination *subsystem* and *point code* (PC+SSN) that actually processes the GT, it can provide a *final GTT*. Such an SP is called a *final TSP* (FTSP).

If a TSP only has knowledge of another TSP that provides further GTT actions (i.e., data needed to forward the GT toward its ultimate PC+SSN), it can only provide an *intermediate GTT*. Such an SP is called an *intermediate TSP* (ITSP).

- An *SCCP route destination* is the recognized signaling point to which a GT is sent for final processing (destination PC+SSN), or further GTT action and forwarding toward the final destination (a TSP). A *primary* SCCP route destination is the preferred TSP or destination PC+SSN; a *secondary* (or *backup*) SCCP route destination can be defined, but is used only if the primary route destination is prohibited (unavailable).
- For a 5ESS[®]-2000 switch GSM, *local GTTs* may be provisioned. This refers to a detailed mapping of one or more digits in a called party address for a specific application (i.e., a TT) to an SCCP route destination. Because the SCCP route destination can be a TSP only or the final PC+SSN, the GSM can act as an ITSP or FTSP, respectively.

GSMs can also provision *remote GTTs*, where local analysis of called party address digits are not required. In this case, all GTs associated with a particular application (i.e., TT) are forwarded to an SCCP route destination corresponding to a TSP, which has the knowledge to perform a GTT to forward the message toward its final destination. In this case, the GSM is not really performing any GTT, but is acting as a relay.

All GTs originating in the GSM must be sent to SCCP route destinations explicitly provisioned. The GTTs performed within the GSM always direct messages to a *primary* SCCP route destination. However, it is possible to provision *mutual alternate SCCP destinations* (as primary/backup pairs). If either SCCP destination is specified by a GTT, and that destination is prohibited or inaccessible, the alternate destination in the pair is used as backup.

For more details about SCCP provisioning on the GSM, see "SCCP Provisioning," Section 13.3.

With this background, the topic of SRVT can be considered. The primary goal of the SRVT mechanism is to send test messages from the GSM for a particular GT (TT plus called party address digits) to every provisioned primary/secondary SCCP route destination. If that destination is a TSP, test messages are again propagated over every provisional primary/secondary SCCP route destination, as dictated by resident GTT activity. This process is repeated until the final destination (PC+SSN) that processes the GT is reached. If that final destination does indeed have the ability to process the GT, it sends an acknowledgment back through the TSPs and ultimately to the GSM. This ensures that the GT is properly translated, regardless of the SCCP route used. It should be noted that SRVT does not concern itself with the actual MTP routes taken between the GSM, various TSPs, and the final GT destination; it is only concerned with "covering" all possible SCCP routes/TSPs involved in the successful GTT.

All TSPs encountered, as well as the final GT destination, must support SRVT functionality for the test to work properly.

SRVT verifies the accuracy and consistency of the *administrable* SCCP routing data and GTT data at the GSM and all TSPs encountered, as well as the final GT destination's ability to process the request. All of this data is static and can be modified by an equivalent recent change mechanism. SRVT does not check *dynamic* characteristics of SCCP routing availability, or the state of any TSP or the final GT destination. Dynamic status, however can affect the results of the test if SCCP routes are inaccessible or TSP/final GT destination processor outages occur.

SRVT uses three types of OMAP messages (with some variants):

- (1) The SCCP routing verification test (SRVT) message initiates the test of administrable SCCP routing data/final

destination GT processing at any SP that receives it. The *SRVT* message can be partitioned into three types, corresponding to their testing role:

- The *request* form of the message (*SRVT-R*) is sent by a signaling point to request a GTT. The destination of this message is always a TSP.

It is likely that the GSM initiates an *SRVT* session by sending such a message (if it is provisioned as an ITSP for a particular GT, or has remote GTT provisioned for a TT).

If more than one TSP is required to complete GTT activity necessary to identify the final GT destination, an ITSP also sends an *SRVT-R* message to the next ITSP or FTSP.

- The *verify* form of the message (*SRVT-V*) is only sent from an FTSP to one or two final destination SPs that process the GT. The message requests that the recipient verify that the primary/secondary PC+SSN agrees with its database, and that the SSN exists and is capable of processing the associated GT. The GSM itself can be an FTSP.
- The *compare* form of the message (*SRVT-C*) is sent by a TSP to its mate TSP (if the TSP is a member of a mated pair). The purpose of the message is to compare GTT mappings for the associated GT, which should be identical in mated TSP pairs.

All *SRVT* messages contain global title information (the tested *translation type* and *digit* string), and the point code of the initiator (i.e., the OPC of the GSM). The maximum number of translations that can occur before reaching a final GT destination is included (can be specified by craft personnel at the GSM), as well as a *trace request flag*, which indicates whether craft personnel have requested that a *TSP trace list* be sent from a final GT destination to the originating GSM. It also contains the *trace list* of preceding *TSPs* crossed prior to sending the next *SRVT* message. In the *compare variant*, translations for primary/secondary SCCP routes are included.

To avoid confusion, when used by itself, *SRVT* refers to the entire test mechanism, while actual messages are denoted as *SRVT* messages (usually *SRVT-R*, *SRVT-V*, or *SRVT-C*).

- (2) The SCCP routing verification acknowledgment (*SRVA*) message acknowledges each *SRVT* message received, and it encodes a summary of partial test results.
- (3) The SCCP routing verification result (*SRVR*) message is sent from the final GT destination or an intermediate TSP back to the initiating GSM. This can be a normal SCCP route trace from the final GT destination; or errors reported by any TSP crossed in the test, a tested mate TSP, or the final GT destination.

In SCCP routing verification testing, all signaling points in a valid route between the GSM and final GT destination, inclusive, actively participate in the test; this also includes a TSP's mate, if applicable. These *SRVT* messages are spawned:

- The initiating GSM sends *SRVT* messages to each *SCCP route destination* provisioned for the target GT.

Normally, these are *SRVT-R* messages if the GSM is acting as an ITSP for the tested GT or has remote GTT provisioned. Rarely, *SRVT-V* messages are sent if the full GTT is performed on the GSM. See "SCCP Provisioning," Section 13.3, to survey the types of GTT/SCCP route destination provisioning that are possible in the GSM.

- A TSP receiving an *SRVT-R* message from the GSM checks its own static GTT/SCCP routing data and sends *SRVT* messages to another SP (an *SRVT-R* to another TSP, or *SRVT-V* to the final GT destination). If the TSP is a member of a mated pair, an *SRVT-C* message is also sent to the mate.

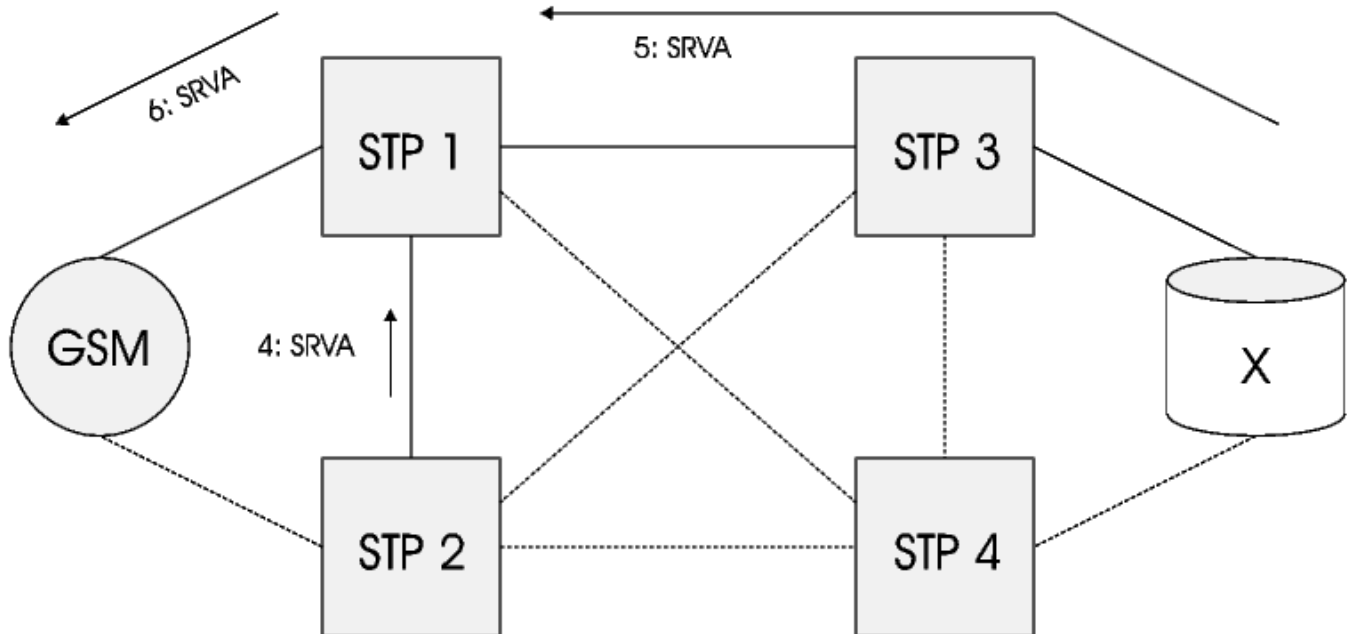


Figure 12.5-13 Typical SRVA Message Flow

The numbers 4, 5, and 6 indicate the order of message generation (based on MTP route length). SRVA 6 is not sent until SRVAs 4 and 5 are received because SRVA 6 represents a composite acknowledgment from STP 1, which includes responses to SRVT 2 and SRVT 3 messages generated. If a *trace* SRVR (described in Section 12.5.3.3.3) is sent from the final GT destination X, it is sent directly to the GSM before SRVA 5 is generated. This is very similar to MRVT/MRVA/MRVA message flow.

The example in Figures 12.5-12 and 12.5-13 is not only very simplistic, but is also a fault-free scenario. If all the SRVT messages generated result in successful SRVA messages being returned, the craft personnel initiating the test on the GSM would be notified that all GTT activity associated with the tested GT is working properly. Thus far, error cases have not been considered, and finding GTT/SCCP routing errors is the primary purpose of the SRVT mechanism. In fact, SRVT should be initiated when GTT/SCCP routing faults are likely to occur:

- (1) Whenever new GTTs are provisioned (see the procedures "Define GTT Translation Groups with Non-Fixed Digit Strings," Section 13.3.4, "Define GTT Translation Groups with Fixed Digit Strings," Section 13.3.5, "Define Single GTT with Non-Fixed Digit Strings," Section 13.3.11, and "Define Single GTT with Fixed Digit Strings," Section 13.3.12 for *local* GTTs, and "Define SCCP Translation Table," Section 13.3.6, for *remote* GTTs).
- (2) Whenever a GTT is modified, or backup SCCP route destinations are altered (see procedures "Update Single GTT with Non-Fixed Digit Strings," Section 13.3.13, or "Update Single GTT with Fixed Digit Strings," Section 13.3.14 for *local* GTTs, "Update SCCP Translation Table," Section 13.3.15 for *remote* GTTs, and "Update Backup SCCP Route Destinations," Section 13.3.9 for changes to backup SCCP route destinations).
- (3) Whenever a problem is suspected in a GTT, as a result of network surveillance or as a result of a customer trouble report.

In these error cases, craft personnel are provided with useful information about the exact nature of GTT/SCCP routing errors on the local GSM, intermediate TSP, or the final GT destinations. These errors are passed back to the initiating GSM by embedded failure data in the SRVA message, and by SRVR messages. Such cases are discussed in detail in other subsections.

The remaining SRVT subsections are decomposed as follows:

- Section 12.5.3.3.2 contains a description of the `EXC:CCS-SRVT` input message, with emphasis on choosing appropriate input parameters for the desired SRVT execution.
- Section 12.5.3.3.3 contains a description of the `EXC CCS-SRVT` and `REPT CCS-SRVR` output messages, noting the types of messages produced in successful and failed SRVT scenarios, and discussing error codes in more detail than the 235-600-750, *5ESS®-2000 Switch Output Message Manual*.
- Section 12.5.3.3.4 provides examples of various successful SRVT scenarios, including input/output message contents, as well as OMAP message flow between signaling points.
- Section 12.5.3.3.5 provides examples of various types of SRVT failures, illustrating input/output message contents, as well as OMAP message flow between SPs.

12.5.3.3.2 SRVT Input Message Formats

In the 5ESS®-2000 switch, SCCP routing verification testing is initiated on GSM PSU signaling platforms (in 5E13 and later software releases) with the `EXC:CCS-SRVT` command.

The simplest format is:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c
```

where *a* is the translation type (TT) in the range 0-255 of the GT under test, *b* represents the digits in the GT called party address to be translated (1-24 characters in length), and *c* is the 9-digit OPC of the target GSM. This format restricts the maximum number of *TSPs crossed* during the test to the default value of 2, not including the GSM itself (if it is provisioned for remote GTT processing) or the final GT destination.

To specify a different number of TSPs that can be crossed, the input message is:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c,NTSP=d
```

where *d* is the number of TSPs that can be crossed in any tested path (in the range 1-15). This number represents only signaling points where *translations* are actually *performed* to move *SRVT* messages *toward* their final GT destination; it does not include TSPs in mated pairs, checked via the *compare variant* of the *SRVT* message.

To specify the only TSP to which the GSM initiator can send the *SRVT* message:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c,TPC=e
```

where *e* is the 9-digit translation point code (TPC), which is the first TSP to which the *SRVT* should be sent. If this option is used, the only requirement within the GSM is that the TPC specified is provisioned as a DPC. The *SRVT* is sent to the TPC directly, bypassing any GTT action or known SCCP route destination data in the GSM (if provisioned). This is useful in verifying *remote GTT* processing before it is actually provisioned, or to restrict provisioned remote GTT processing to either primary or backup SCCP route destination (if provisioned). This option should *not* be used if the GT under test is provisioned for *local GTT* because the *SRVT* does not reflect normal processing and may lead to a false conclusion.

If the TPC option is not specified, the default is to determine the primary (and possibly, backup) SCCP route destinations from provisioned data. This could be the result of *local GTT* processing (intermediate or final), or the more common *remote GTT* processing based only on TT.

For either of the above cases, if the primary SCCP route destination to a TSP/final GT destination is provisioned

with a *backup* route destination, an *SRVT* is also sent to the backup destination.

It is possible to request a *trace list* of *TSPs crossed* for all possible paths used in the *SRVT* session. The final GT destination must be reached successfully because this SP sends the trace information to the GSM for output. This form is:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c,TRACE
```

The *NTSP*, *TPC*, and *TRACE* options can be mixed and matched.

An *SRVT* request may not be able to start because of local conditions in the office/GSM, such as:

- the *OPC* specified is not for any provisioned GSM,
- the *OPC* is specified in an invalid format,
- the GSM is not available (isolated or initializing),
- the specified *TPC* is invalid (not a *DPC* provisioned for the GSM) or the *TPC* is actually the GSM's *OPC*,
- the GT (*TT* and *DIGITS*) is not provisioned *SCCP* data on the GSM,
- the GT is already under test on the target GSM (duplicate *TT*, *DIGITS*, and *OPC*),
- the *TPC* is inaccessible,
- the GSM cannot process *SCCP* messages because the intra-SM MD path is OOS,
- or the maximum number of *SRVTs* is already running (this limit is provisionable, as described in "Operation, Maintenance and Administration Part Provisioning," Section 13.1.22).

See the 235-600-700, *5ESS®-2000 Switch Input Message Manual* and the 235-600-750, *5ESS®-2000 Switch Output Message Manual* for more details and the exact outputs produced in these cases.

12.5.3.3.3 *SRVT* Output Message Formats

There are four types of *SRVT* output messages possible in fault-free scenarios.

The first output message produced indicates that the *SRVT* session has started.

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST STARTED
TPC: d
MAX GTT ALLOWED: e
TRACE REQUESTED
```

where *a* is the translation type (*TT*) of the GT to be analyzed, *b* represents the called party address digits in that GT, *c* is the 9-digit *OPC* of a specific GSM, and *e* is the maximum number of *TSPs* that can be crossed during testing (the number entered on the input command, or the default value of 2). *TRACE REQUESTED* indicates that craft personnel requested a *trace* of *TSPs* crossed (NO *TRACE REQUESTED* is output if no trace is requested). The variable *d* indicates the *initial TPC(s)*, to which *SRVTs* are sent by the GSM. This is the *TPC* specified in the input message, or the *default* selected by the GSM, if none was specified by craft personnel. The default is the *TSP* (or possibly a pair of primary/secondary *SCCP* destinations) determined by local *GTT* analysis or remote *GTT* provisioning.

The next group of messages provides the results of *each SRVA* returned to the GSM (in response to each *SRVT*

message sent), with "complete success" implied at this point.

```
EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS
SRVA RECEIVED FROM: f
SRVA RESULT: SUCCESS
```

where *f* is the 9-digit translation signaling point (TSP) or final GT destination returning the *SRVA* message to the GSM. The *SUCCESS* qualifier on the first line refers to the results of the entire test spawned; the result in the third line refers to the individual *SRVA* reported.

Another type of message is possible if the *TRACE* option is included in the input command:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS
TRACE SRVR FROM: g
NUMBER OF TSPS CROSSED: h
TRACE LIST:
i .....
```

The *SRVR* messages with the *trace list* are produced only by the final GT destinations; both *primary* and *secondary* final GT destinations can produce these *SRVRs*, and one is returned for each separate SCCP route used. The final GT destination sending the *SRVR* is *g* (9-digit point code); the number of TSPs crossed is *h* (which excludes the GSM if provisioned for *remote GTT*, and the final GT destination); and the actual trace list is *i*, which may identify up to eight 9-digit TSPs (in multiline format). When an *SRVT-C* message is sent to check the mate of a TSP pair, the point code of the mate is also included in that trace list.

The last message received, after all *SRVA* reports and optional *SRVR* traces are produced, is:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST ENDED
```

Departing from the above fault-free scenario, a variety of failures or partial success conditions can occur.

The output messages reporting *SRVA* results have a more flexible format:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c j
SRVA RECEIVED FROM: f
SRVA RESULT: k
ERRORS DETECTED:
m
```

where *j* is the summary result for the entire *SRVT* session spawned by the GSM (values selected from *PARTIAL SUCCESS* or *FAILURE*, under the assumption of a faulty scenario); and *k* is the result returned by a particular *SRVA*, selected from *SUCCESS*, *PARTIAL SUCCESS*, or *FAILURE* (for faulty scenarios, at least one *SRVA* must be a *PARTIAL SUCCESS* or *FAILURE*).

If an *SRVA* is a *PARTIAL SUCCESS* or *FAILURE*, one or more error conditions *m* are listed (on multiple lines if necessary). The *ERRORS DETECTED* line is omitted and *m* is blank if the *SRVA* result is *SUCCESS*.

The *SRVR* error codes are listed in Table 12.5-3 .

Table 12.5-3 SRVR Error Codes

Error Code	Description
LOOP	A <i>loop</i> is detected if the next TSP to which an <i>SRVT</i> message would normally be sent already exists in the <i>trace list</i> received. The <i>SRVT</i> message received by a TSP always contains a trace of previous TSPs traversed. When a <i>compare SRVT</i> is sent to a mate in a

	TSP mated pair, the point code of the mate is also added to the trace list. A similar failure occurs if an attempt is made by a TSP to send an <i>SRVT</i> message back to the initiating GSM's OPC.
EXCESSIVE LENGTH ROUTE	The number of point codes in the <i>trace list</i> in a received <i>SRVT</i> message is generally twice the number of TSPs performing GTTs traversed thus far (because the point codes of both TSPs in a mated pair are included in trace list, even though only one is traversed). The <i>count of TSPs</i> performing GTTs is then determined by dividing the number of point codes in the trace list by 2 (if the result is not a whole number, it is rounded up). If that count is greater than or equal to the <i>maximum number of GTTs</i> allowed encoded in the message, and this is not the <i>final GT destination</i>, an excessively long route is detected. The maximum GTT allowed parameter defaults to 2 unless the input command on the GSM specifies another value (any value in the range 1-15 is permitted).
NO TRANSLATION FOR GLOBAL TITLE	The TSP receiving an <i>SRVT</i> message has no translation data to propagate the encoded GT (TT plus DIGITS) to another TSP or the final GT destination.
INACCESSIBLE ROUTE	An <i>SRVT</i> message cannot be sent to a TSP or the final GT destination because SCCP access to the associated point code is congested or the point code is inaccessible.
LOCAL CONDITIONS	If a TSP (other than the GSM) cannot continue the <i>SRVT</i> processing for some reason local to its processor or because the maximum number of <i>SRVT</i> messages that the TSP can handle is exceeded, an <i>SRVA</i> with this error condition is returned to the <i>SRVT</i> originator (if possible).
UNKNOWN INITIATING POINT CODE	A TSP or the final GT destination has no knowledge of the initiating GSM's OPC in its MTP routing tables. Routing should be bidirectional. If the GSM's OPC is not a valid SCCP route at a given TSP/final GT destination, it is impossible for that point code to send an <i>SRVR</i> to the GSM to make the problem known. Instead, an <i>SRVA</i> is returned to the originator of the <i>SRVT</i> message with the UNKNOWN INITIATING POINT CODE error, and an indication that no <i>SRVR</i> was sent. The SP receiving this <i>SRVA</i> sends the <i>SRVR</i> message to the initiating GSM, citing pertinent data associated with this error (including the point code that actually has the routing problem).
TIMER EXPIRED	Expected <i>SRVAs</i> are not received within a prescribed time-out interval (so-called T2 timer). This timer in the GSM is calculated dependent upon GT treatment. If the translation type (TT) is only subject to <i>remote GTT</i> processing, the T2 timer is defined as $T2 = D \times (N + 1)$, where N is the number of TSPs performing GTTs that can be crossed, as specified in the input message (or N=2 by default), and D is the delay or expected processing/transmission time for <i>SRVT/SRVA</i> message exchange (this is recent changeable, as described in "Operation, Maintenance and Administration Part Provisioning," Section 13.1.22). If the GT is subject to <i>local GTT</i> processing, the timer is reduced to $T2 = D \times N$ because the GSM's OPC is added to the <i>trace list</i> (reducing by 1 the number of external TSPs that can be traversed).
WRONG SP	An <i>SRVT</i> message arrives at a signaling point that cannot provide the processing implied by the message type. The scenarios related to this type of failure are: - Any SP that is not a member of a mated TSP pair receives an <i>SRVT-C</i> (<i>compare</i> variant). - A member of a mated TSP pair receives an <i>SRVT-C</i> (<i>compare</i> variant) from an SP that is not its mate. - An <i>SRVT-R</i> (<i>request</i> variant) is received by an SP that is not a TSP. - An <i>SRVT-V</i> (<i>verify</i> variant) is received by a TSP or any SP that is not a final GT destination.

INCORRECT TRANSLATION FOR PRIMARY DESTINATION	This error is detected by the mate of a duplex <i>FTSP</i> pair. The <i>primary</i> point code plus SSN of the final GT destination contained in an <i>SRVT-C</i> (<i>compare</i> variant) does not match static data in the detecting <i>FTSP</i> .
INCORRECT TRANSLATION FOR SECONDARY DESTINATION	This error is detected by the mate of a duplex <i>FTSP</i> pair. The <i>secondary</i> point code plus SSN of the final GT destination contained in an <i>SRVT-C</i> (<i>compare</i> variant) does not match static data in the detecting <i>FTSP</i> .
INCORRECT TRANSLATION FOR INTERMEDIATE TSP	This error is detected by the mate of a duplex <i>ITSP</i> pair. The results of an <i>intermediate GTT</i> contained in an <i>SRVT-C</i> (<i>compare</i> variant) do not match similar <i>GTT</i> processing on the detecting <i>ITSP</i> .
NOT PRIMARY DESTINATION	This error is detected by the <i>primary</i> NCP/SCP in a mated pair of final GT destinations, if it does not serve the GT specified in the received <i>SRVT-V</i> (<i>verify</i> variant) as a primary destination. The same error is reported by a non-mated NCP/SCP or SEP office if it does not serve the GT specified in the received <i>SRVT-V</i> message.
NOT SECONDARY DESTINATION	This error is detected by the <i>secondary</i> NCP/SCP in a mated pair of final GT destinations, if it does not serve the GT specified in the received <i>SRVT-V</i> (<i>verify</i> variant) as a secondary destination. The same error is reported by a non-mated NCP/SCP or SEP office if it does not serve the GT specified in the received <i>SRVT-V</i> message.
PRIMARY DESTINATION NOT RECOGNIZED	This error is detected <i>only</i> by the <i>secondary</i> NCP/SCP in a mated pair of final GT destinations when the <i>primary</i> point code plus SSN in a received <i>SRVT-V</i> (<i>verify</i> variant) is not recognized as the primary destination for the target GT. That secondary NCP/SCP, however, <i>does</i> recognize the <i>secondary</i> point code plus SSN as the secondary destination for the GT that it serves.
SECONDARY DESTINATION NOT RECOGNIZED	This error is detected <i>only</i> by the <i>primary</i> NCP/SCP in a mated pair of final GT destinations when the <i>secondary</i> point code plus SSN in a received <i>SRVT-V</i> (<i>verify</i> variant) is not recognized as the secondary destination for the target GT. That primary NCP/SCP, however, <i>does</i> recognize the <i>primary</i> point code plus SSN as the primary destination for the GT that it serves.
ROUTING PROBLEM	This error is detected by a TSP that does not recognize the point code of the SCCP route destination derived from its own <i>GTT</i> analysis.
SUCCESS TO GATEWAY	The <i>SRVT</i> message successfully reaches the gateway intermediate signal point, but is unable to continue the internetwork test.
UNKNOWN ERROR CODE x	Failure codes <i>x</i> above the value of 16 are considered unknown by the GSM.

In the case when routes to the TPC are inaccessible, the GSM cannot send an *SRVT* and a special output format is spawned internally by the GSM:

```

EXC CCS SRVT TT=a DIGITS=b OPC=c j
SRVT NOT SENT
ERROR DETECTED: INACCESSIBLE TPC
POINT CODES AFFECTED:
n

```

where *n* is the translation point code that is inaccessible/congested. Another error type, *NETWORK ERROR*, could be specified in the above format; this corresponds the inability of SCCP to transmit the *SRVT* message to the TPC.

Similarly, for the case in which no *SRVA* is received because of the *TIMER EXPIRED* condition, another type of message is generated internally by the GSM:

```

EXC CCS SRVT TT=a DIGITS=b OPC=c j
SRVA NOT RECEIVED
ERRORS DETECTED: TIMER EXPIRED

```

POINT CODES AFFECTED:

p

where p is the TPC that does not return an SRVA in the time allotted.

When a TSP receives an SRVT message, it normally generates one or more SRVT messages itself to its mate TSP, to another TSP that performs further GTT actions, or to final GT destinations. Before an SRVA can be returned to the originator of the SRVT message received, the TSP must receive all SRVA messages corresponding to SRVT messages sent (or the T2 guard timer at the TSP expired).

Figure 12.5-14 illustrates SRVT/SRVA message flow at a TSP.

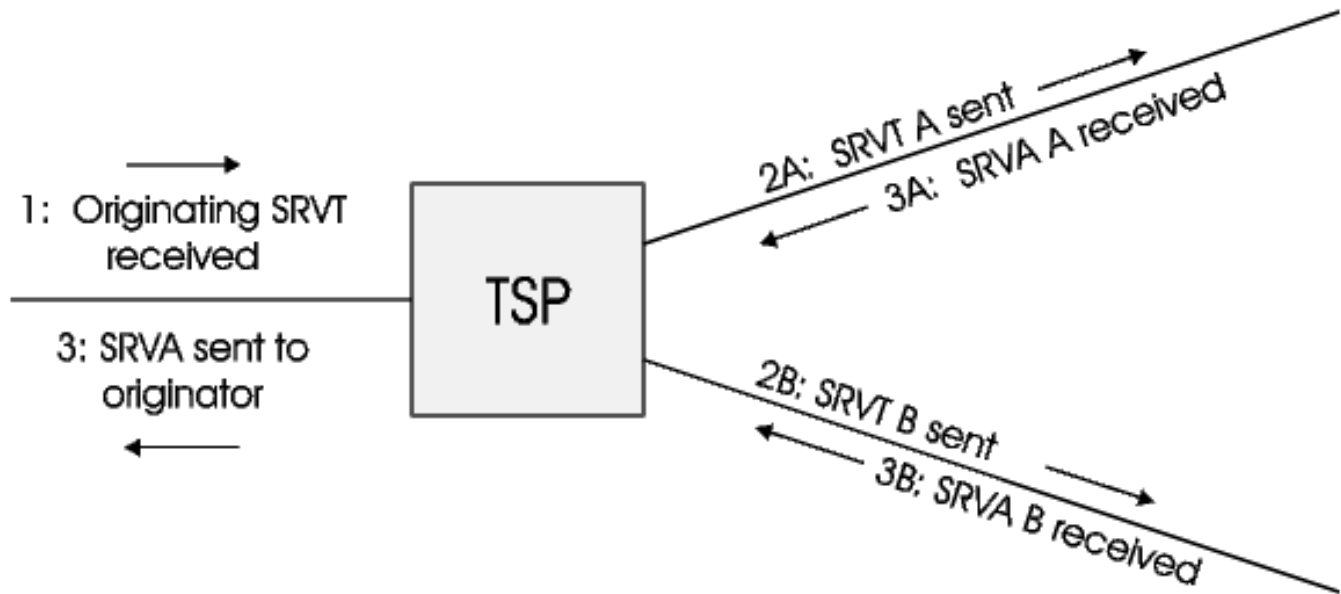


Figure 12.5-14 SRVT / SRVA Message Flow at a TSP

Increasing time is represented by the sequence 1, (2A, 2B), (3A, 3B), 4. If the guard timer expires before all expected SRVA messages are received, the missing SRVAs are considered to be received with a FAILURE result and a TIMER EXPIRED error code. SRVAs received after the timer expires are discarded.

Each of the SRVA messages 3A, 3B received also has a result/possible error code:

- If the result is SUCCESS, all downstream SRVA messages between the specified TSP and the final GT destination have a SUCCESS result.
- If the result is PARTIAL SUCCESS, at least one downstream SRVA message has a SUCCESS result and at least one has a FAILURE result.

Also included is a composite error code, which is a "logical ORing" of all types of errors reported by downstream FAILURE SRVA messages (as described in Table 12.5-3).

- If the result is FAILURE, then all downstream SRVA messages have FAILURE results. The composite error code is also included.

The flow of SRVA processing starts at the final GT destinations (where only SUCCESS or FAILURE results are possible) and passes through intermediate TSPs until SRVA messages are delivered back to the initiating GSM. For

the TSP example in Figure 12.5-14, the results/error codes from *SRVAs* for events 3A and 3B are "logically combined," using the above algorithm, to produce the *MRVA* message in event 4. If the progress is halted at a TSP (the final GT destination is never reached), the *SRVA* backward flow toward the GSM starts at that TSP.

The *SRVA* messages received by the GSM represent the quality of a particular SCCP route in handling a GTT (including operations at intervening TSPs and the final GT destinations). Returned error codes are for one or more SCCP routes used to reach the final GT destinations. *SRVA* message data provides no information about the source (TSP/final destination) of those errors; the *SRVA* responses contain only general error information.

The assumption is that one or more signaling points are experiencing problems. Because *SRVAs* do not contain the signaling point where the error occurred or supplemental information necessary to isolate the problem, more data must be provided to the 5ESS®-2000 switch craft personnel. This additional troubleshooting information is provided by the *SCCP routing verification result (SRVR)* message.

The *SRVR* message is output when the craft personnel request that a *trace list* be returned. This type of supplemental information (i.e., a successful trace) may still be delivered in error conditions, provided *SRVT* messages reach the final GT destination and that signaling point is capable of returning the trace. The only difference is that the overall test result SUCCESS on the first line of output is replaced by PARTIAL SUCCESS.

The more interesting case of detailed error location is supplied by the output message:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c j
SRVR RECEIVED FROM: q
ERROR DETECTED: s
SUPPLEMENTAL INFO:
t
```

where *j* is the overall test result (PARTIAL SUCCESS or FAILURE), *q* is the signaling point where the error is detected (which could be a TSP or a final GT destination), *s* is the error type (listed in Table 12.5-3), and *t* is optional supplemental information, as listed in Table 12.5-4. *Administrative* actions that should be taken in response to *SRVRs* received at the GSM are included in Table 12.5-4 entries.

Such *SRVR* messages are delivered directly from the SP detecting the error to the initiating GSM, via the preferred SCCP route. There is one exception for the UNKNOWN INITIATING POINT CODE case, which is described in the appropriate Table 12.5-4 entry.

In addition to *SRVRs* sent, the TSP/final GT destination returns a PARTIAL SUCCESS or FAILURE *SRVA* message to the originator of the *SRVT* that contains a composite of error codes detected. Also, TSPs that detect the error generally cease propagating any other downstream *SRVT* messages. There are exceptions, such as the results of *compare SRVT* messages, or as noted in Table 12.5-4.

Table 12.5-4 Supplemental *SRVR* Error Information

Error Code	Supplemental Information/Administrative Actions
LOOP	For the detected loop, the TSP that would route an <i>SRVT</i> message to another TSP already in the trace list is identified as the <i>q</i> parameter in the <i>SRVR</i> . The list of SPs involved in the potential loop is provided as supplemental information <i>t</i> (this is the trace list in the received <i>SRVT</i> message, plus the TSP that detects the error, plus the TSP indicated by the GTT results that would have been created the loop). A detected routing loop must be resolved administratively. GTT data on the TSP that would have been created the loop, as well as the duplicate SP identified, are suspect.
EXCESSIVE LENGTH ROUTE	If a TSP does not provide a final GTT, and the number of TSPs in the trace list indicates the maximum number of GTTs allowed has been reached, an excessive length route has been detected. The <i>SRVR</i> parameter <i>q</i> is the TSP that detects the excessive route length

	and τ contains the trace list. If the number of TSPs crossed is of great importance, the only alternative is to redefine SCCP route destinations at the GSM. Another possible scenario is that the test was executed with a default value of 2 GTTs allowed. If a longer route can be tolerated, re-execute the <code>SRVT</code> command, but increase the <code>NTSP</code> parameter and specify the <code>TRACE</code> option. If the SCCP route of interest is longer but viable, perhaps no administrative changes are required.
NO TRANSLATION FOR GLOBAL TITLE	In this case, a TSP has no translation data to handle the received GT. The TSP that detects the error is identified in the <code>SRVR</code> parameter n, and the current trace list is provided as supplemental information τ (the GSM or last TSP in the trace list that sent the <code>SRVT</code> to the TSP detecting the error may be at fault). If an <code>SRVT-R</code> message is sent to a TSP that does not serve the tested GT, the problem can be the originator of the <code>SRVT</code> (data in that signaling point directs the <code>SRVT</code> to the wrong SCCP destination), or the receiving TSP (the tested GT should be translated on that TSP). Administrators of both involved signaling points must decide on the appropriate action.
INACCESSIBLE ROUTE	The SCCP route destinations required to propagate <code>SRVTs</code> are inaccessible or congested. The <code>SRVR</code> parameter n contains the SP that detects the error, and supplemental information q contains a list of downstream PCs that cannot be reached because of the inaccessible or congested routes. In addition to the <code>SRVR</code> sent, the SP that detects the error returns an <code>SRVA</code> with the INACCESSIBLE ROUTE error code to the originator of the <code>SRVT</code>, but further downstream <code>SRVT</code> processing ceases on the <i>affected routes only</i>. If the GSM detects this situation, equivalent error messages are internally generated. This is an error caused by <i>dynamic states</i> of an SCCP route. It is transient in nature (it is assumed that administrators of the affected signaling points are actively attempting to correct the problem), and the <code>SRVT</code> command should be re-executed at a later time when the problem is resolved.
LOCAL CONDITIONS	<code>SRVT</code> analysis/propagation must cease because of local problems at a TSP. If the TSP has enough sanity/real-time to send an <code>SRVR</code>, the TSP with the local problem is identified in the parameter q (this is duplicated as supplemental information τ). This is a <i>dynamic problem</i>, <code>SRVT</code> command should be retried later.
UNKNOWN INITIATING POINT CODE	A TSP or final GT destination has no knowledge of the GSM's OPC in its MTP routing tables, so the <code>SRVR</code> that should be generated cannot be delivered to the GSM. Instead, all further downstream <code>SRVT</code> processing ceases (if applicable), and the FAILURE <code>SRVA</code> with the UNKNOWN INITIATING POINT CODE error is sent to the <code>SRVT</code> originator; this <code>SRVA</code> has a special indication that <i>no SRVR was sent</i>. Upon receipt of such an <code>SRVA</code>, the receiving SP sends the <code>SRVR</code> to the GSM. <code>SRVR</code> parameter q is the SP that generates the <code>SRVR</code> and τ is the point code that has no knowledge of the initiating GSM. SCCP routing should be bidirectional, so appropriate routing data should be provisioned on the signaling point without knowledge of the initiating GSM. Another possible scenario is that the GSM itself directed an <code>SRVT</code> message to the wrong TSP (this is compounded by the possible incorrect use of the TPC on the <code>EXC:CCS</code>, <code>SRVT</code> command).
TIMER EXPIRED	One or more expected <code>SRVAs</code> are not received before the T2 guard timer expires (described in Table 12.5-3). The detecting TSP sends an <code>SRVR</code> to the GSM, with parameter q being the TSP detecting the expired timer and τ a list of signaling points that

	do not return the <i>SRVA</i>. If the GSM detects this problem, an equivalent error message is internally generated. A TSP detecting the time-out also sends an <i>SRVA</i> with <i>TIMER EXPIRED</i> error to the <i>SRVT</i> originator. The <i>SRVA</i> returned can contain other error codes because some <i>SRVAs</i> at the TSP/GSM may be received on time. Missing <i>SRVAs</i> triggering the time-out that are received later are discarded by the TSP/GSM. Because the cause of this problem is probably dynamic in nature, an <i>SRVT</i> retry is justified.
WRONG SP	An <i>SRVT</i> message is received at a signaling point that cannot provide the required processing for the <i>SRVT</i> type (request, verify, or compare). The parameter <i>q</i> in the <i>SRVR</i> sent is the signaling point detecting the problem, and supplemental information <i>t</i> contains the trace list of crossed TSPs leading to the SP detecting the problem. This is a critical problem that must be resolved. The likely cause is the TSP sending the <i>SRVT</i>, when GTT analysis results in an erroneous SCCP route destination. A less likely cause is that the mated TSP pairs have no knowledge of their mate.
INCORRECT TRANSLATION FOR PRIMARY DESTINATION	The primary GT destination derived from GTT analysis in a mated pair of FTSPs does not agree. The <i>SRVR</i> parameter <i>q</i> is the mate FTSP receiving the <i>SRVT-C</i> message, and supplemental information <i>t</i> contains a TSP trace list, the last point code of which is the member of the FTSP pair sending the <i>SRVT-C</i> message. Administrators must ensure that consistent GTT data is maintained on the cited FTSP mated pair.
INCORRECT TRANSLATION FOR SECONDARY DESTINATION	The secondary GT destination derived from GTT analysis in a mated pair of FTSPs does not agree. The <i>SRVR</i> parameter <i>q</i> is the mate FTSP receiving the <i>SRVT-C</i> message, and supplemental information <i>t</i> contains a TSP trace list, the last point code of which is the member of the FTSP pair sending the <i>SRVT-C</i> message. Administrators must ensure that consistent GTT data is maintained on the cited FTSP mated pair.
INCORRECT TRANSLATION FOR INTERMEDIATE TSP	The results of an intermediate GTT in mated pair of ITSPs differ. The <i>SRVR</i> parameter <i>q</i> is the mate ITSP receiving an <i>SRVT-C</i> message, and supplemental information <i>t</i> contains a TSP trace list, the last point code of which is the point code of the ITSP pair sending the <i>SRVT-C</i>. Administrators must ensure that consistent GTT data is maintained on the cited ITSP mated pair.
NOT PRIMARY DESTINATION	The primary NCP/SCP in a mated pair of final GT destinations (or a non-mated NCP/SCP or SEP office) does not serve the GT specified in a received <i>SRVT-V</i> message as a primary destination. The <i>SRVR</i> parameter <i>q</i> is the signaling point detecting the condition, and supplemental information <i>t</i> contains a TSP trace list, the last point code of which is the FTSP sending the errored <i>SRVT-V</i> message. This error represents a critical data problem. Either the subsystem on the identified final GT destination reporting the error must be enhanced to process the tested GT, or the FTSP sending the <i>SRVT-V</i> message must alter GTT data to provide another SCCP destination. Administrators of both nodes should be involved.
NOT SECONDARY DESTINATION	The secondary NCP/SCP in a mated pair of final GT destinations (or a non-mated NCP/SCP or SEP office) does not serve the GT specified in a received <i>SRVT-V</i> message as a secondary destination. The <i>SRVR</i> parameter <i>q</i> is the signaling point detecting the condition, and supplemental information <i>t</i> contains a TSP trace list, the last point code of which is the FTSP sending the errored <i>SRVT-V</i> message. Administrative actions are identical to the NOT PRIMARY DESTINATION error.

PRIMARY DESTINATION NOT RECOGNIZED	A secondary NCP/SCP in a mated pair of final GT destinations does not recognize the primary point code plus SSN supplied in an <i>SRVT-V</i> message from an FTSP. The <i>SRVR</i> parameter <i>q</i> identifies the final GT destination detecting the error, and supplemental information <i>t</i> contains a TSP trace list, the last point code of which is the FTSP sending the <i>SRVT-V</i> message. The likely cause is the TSP sending the <i>SRVT</i>, when GTT analysis results in an erroneous SCCP primary route destination. A less likely cause is that the mated pairs of primary/secondary GT destinations have incorrect data.
SECONDARY DESTINATION NOT RECOGNIZED	A primary NCP/SCP in a mated pair of final GT destinations does not recognize the secondary point code plus SSN supplied in an <i>SRVT-V</i> message from an FTSP. The <i>SRVR</i> parameter <i>q</i> identifies the final GT destination detecting the error, and supplemental information <i>t</i> contains a TSP trace list, the last point code of which is the FTSP sending the <i>SRVT-V</i> message. The likely cause is the TSP sending the <i>SRVT</i>, when GTT analysis results in an erroneous SCCP secondary route destination. A less likely cause is that the mated pairs of primary/secondary GT destinations have incorrect data.
ROUTING PROBLEM	A TSP does not recognize the point code of the SCCP route destination derived from its own GTT analysis. The <i>SRVR</i> parameter <i>q</i> is the TSP detecting the problem, and supplemental information <i>t</i> contains a TSP trace list. This is a critical problem that must be resolved. The TSP reporting the problem has erroneous GTT data resulting in a translation to an unknown SCCP destination, or the SCCP destination itself must be made known to routing.
SUCCESS TO GATEWAY	This error implies that a gateway intermediate signaling point receives an <i>SRVR</i>, but further <i>SRVT</i> analysis is impossible. The <i>SRVR</i> parameter <i>q</i> contains the point code of the gateway SP detecting the problem, and <i>t</i> contains the trace list leading to that SP.
UNKNOWN ERROR CODE x	If a non-Lucent Technologies[®] SP detects an unrecognized error (code <i>x</i>), the <i>SRVR</i> parameter <i>q</i> contains the point code reporting the error (supplemental information <i>t</i> duplicates this point code). The administrator of the signaling point returning such an error must be contacted to determine whether or not the reported error affects operations.

When a TSP or final GT destination receives an *SRVT* message, the processing of *SRVRs*/*SRVAs* proceeds in this sequence:

- (1) If the receiving TSP/final GT destination cannot process the *SRVT* any further because of local conditions (see Table 12.5-4), *SRVR*/*SRVA* messages are immediately generated with the LOCAL CONDITIONS error code, and further *SRVT* processing ceases.
- (2) If the test can proceed, it is verified that the initiating GSM's OPC is known. If the OPC is *not* known, then an *SRVA* message is immediately generated with UNKNOWN INITIATING POINT CODE error code, and further *SRVT* processing ceases. This is not possible at a TPC associated with the GSM.
- (3) If a TSP or final GT destination receives an *SRVT* of a type (request, verify, or compare) that is *not* compatible with its functionality, *SRVR*/*SRVA* messages are immediately sent with the WRONG SP error code, and further *SRVT* processing ceases.
- (4) If the initiating GSM's OPC is known, it is determined if the TSP receiving the *SRVT* has no GTT data to translate the tested GT. If so, *SRVR*/*SRVA* messages are immediately generated with the NO TRANSLATION FOR GLOBAL TITLE error code, and further *SRVT* processing ceases.

This case is not valid for final GT destinations.

- (5) If a TSP passes the above checks, it is verified that SCCP routing loops are not generated and that no excessive route length is detected (see Table 12.5-4 for details). If so, *SRVR/SRVA* messages with the appropriate LOOP or EXCESSIVE LENGTH ROUTE error specified are immediately generated, and further SRVT processing ceases.

These checks are not valid at final GT destinations.

- (6) If the above checks pass at an *ITSP only* that is also a member of a mated pair, and the result of a comparison the intermediate GTT is different (via an *SRVT-C* message probe), the mate detecting the problem sends an *SRVR/SRVA* message with the INCORRECT TRANSLATION FOR INTERMEDIATE TSP error.
- (7) If the defensive checks [1-5] pass at an *FTSP only* that is also a member of a mated pair, and the result of a comparison the final GTT is different (via an *SRVT-C* message probe), the mate sends *SRVR/SRVA* messages with the INCORRECT TRANSLATION FOR PRIMARY DESTINATION or INCORRECT TRANSLATION FOR SECONDARY DESTINATION error (as appropriate) immediately.
- (8) If defensive checks [1-5] pass at an ITSP/FTSP, and an SCCP route destination specified by an intermediate/final GTT is not known to the TSP, *SRVR* messages with the ROUTING PROBLEM error specified are immediately sent, and further SRVT processing ceases. SRVT processing on a second SCCP route is still possible.
- (9) If a TSP encounters no errors listed above, dynamic routing is polled for any SCCP route destination specified by a successful GTT. If any inaccessible or congested routes are detected, *SRVR* messages with the INACCESSIBLE ROUTE error specified are immediately sent, and further SRVT activity using the *identified routes only* ceases. The *SRVA* ultimately returned contains a composite of the inaccessible route, as well as error responses from any *SRVT* messages successfully sent. The GSM may similarly verify the inaccessibility of a TPC, and equivalent error messages are internally generated.
- (10) In the absence of all problems listed above in a TSP, an *SRVT* message is spawned downstream to ultimately reach the final GT destination. A T2 guard timer (see Table 12.5-3) is set to monitor *SRVA* responses. If the timer expires, an *SRVR* message with the TIMER EXPIRED error is sent for *all SRVAs* not received (if any fail to arrive); an *SRVA* is sent back to the *SRVT* originator with a PARTIAL SUCCESS or FAILURE result, and the TIMER EXPIRED failure code included.

Such a timer is also set in the GSM (whether or not it is providing TSP functionality), and equivalent error messages are internally generated.

- (11) If all the above checks pass at a final GT destination (only those that are appropriate), it is verified whether the tested GT can be processed by the subsystem specified in the *SRVT-V* message. If *not*, an *SRVR* message with the NOT PRIMARY DESTINATION or NOT SECONDARY DESTINATION error specified (as appropriate) is sent. Also, in mated pairs of primary/secondary GT destinations verifies the "point code plus subsystem" data delivered in an *SRVT-V* message is consistent with local data. If data *is inconsistent*, an *SRVR* message with PRIMARY DESTINATION NOT RECOGNIZED or SECONDARY DESTINATION NOT RECOGNIZED error (as appropriate) is sent. *SRVAs* with all errors found are then sent to the originator of the *SRVT* message.

Any *SRVA* or *SRVR* messages that arrive at the GSM after the T2 guard timer expires for a specific test are discarded.

12.5.3.3.4 Successful SRVT Scenarios

This section presents four examples of successful SRVT sessions. They are varied to illustrate the different modes

of global title (GT) processing that can be provisioned in the GSM (FTSP functionality, ITSP functionality, or remote GTT processing), typically a quad-STP architecture of the external network (providing either ITSP and/or FTSP functionality or simply acting as an MTP transport vehicle), and various types of final GT destinations (another SEP office, simplex or duplex/mated or non-mated NCP/SCP database platforms).

For SRVT Example 1 of a successful SRVT session, consider a GSM (OPC=c) that is provisioned to perform *final global title translation (GTT)* for the tested GT (TT=a, DIGITS=b). The primary GT destination is another signaling endpoint (SEP) office, and craft personnel request that a *trace list* be produced. This network architecture is illustrated in Figure 12.5-15, with test message flow indicated (message numbers indicate their likely order of generation in time).

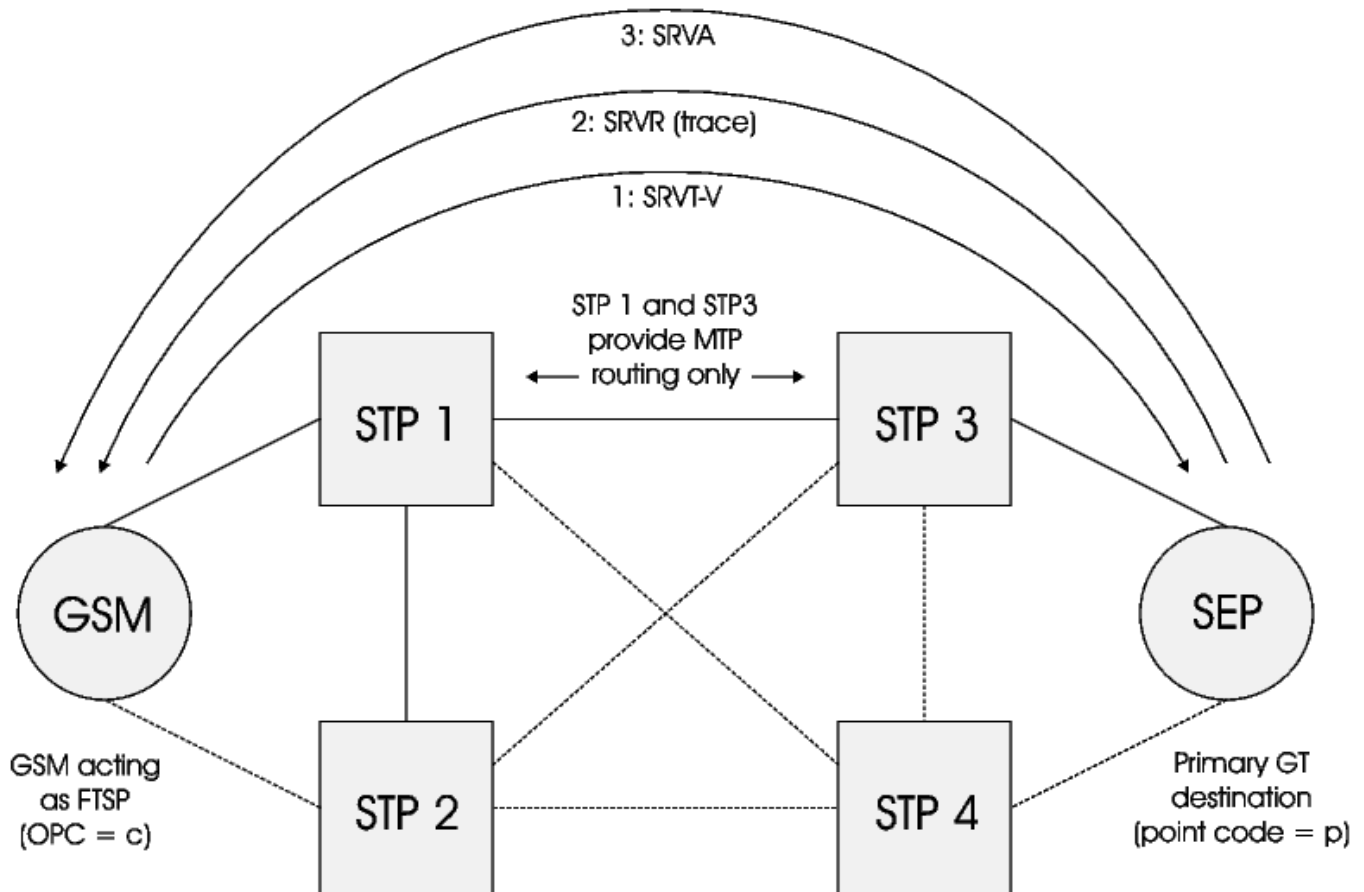


Figure 12.5-15 SRVT Example 1

For the example, craft personnel issue this command on the 5ESS[®]-2000 switch containing the target GSM:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c,TRACE
```

As the GSM performs final GTT analysis (i.e., it derives the point code plus subsystem of the primary GT destination directly), it sends a *verify SRVT* variant directly to the primary GT destination. The intervening quad-STP platform performs no GT translation (GTT) in this case, and acts solely as an MTP transport mechanism.

The output messages produced at the GSM for this test are:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST STARTED
TPC: p
MAX GTT ALLOWED: 2
```

TRACE REQUESTED

EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS

SRVA RECEIVED FROM: p

SRVA RESULT: SUCCESS

EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS

TRACE SRVR FROM: p

NUMBER OF TSPTS CROSSED: 1

TRACE LIST:

c

EXC CCS SRVT TT=a DIGITS=b OPC=c TEST ENDED

The parameters *c* and *p* represent the 9-digit point codes of the GSM's OPC and primary GT destination, respectively. The trace list produced includes the GSM's OPC (point code *c*) because it is providing translation signaling point (TSP) functionality.

In SRVT Example 2, the GSM (with OPC *c*) is provisioned to provide *intermediate GTT* on the specified GT (TT=*a*, DIGITS=*b*). A mated pair of TSPs (STP 3 and STP 4) in the network provides final GTT analysis; the GSM is provisioned to use STP 3 only as an SCCP route destination for the target GT. The final GT destination is a single NCP (primary destination with point code *p*). A trace list is requested by craft personnel. This network architecture is illustrated in Figure 12.5-16 , with test message flow indicated.

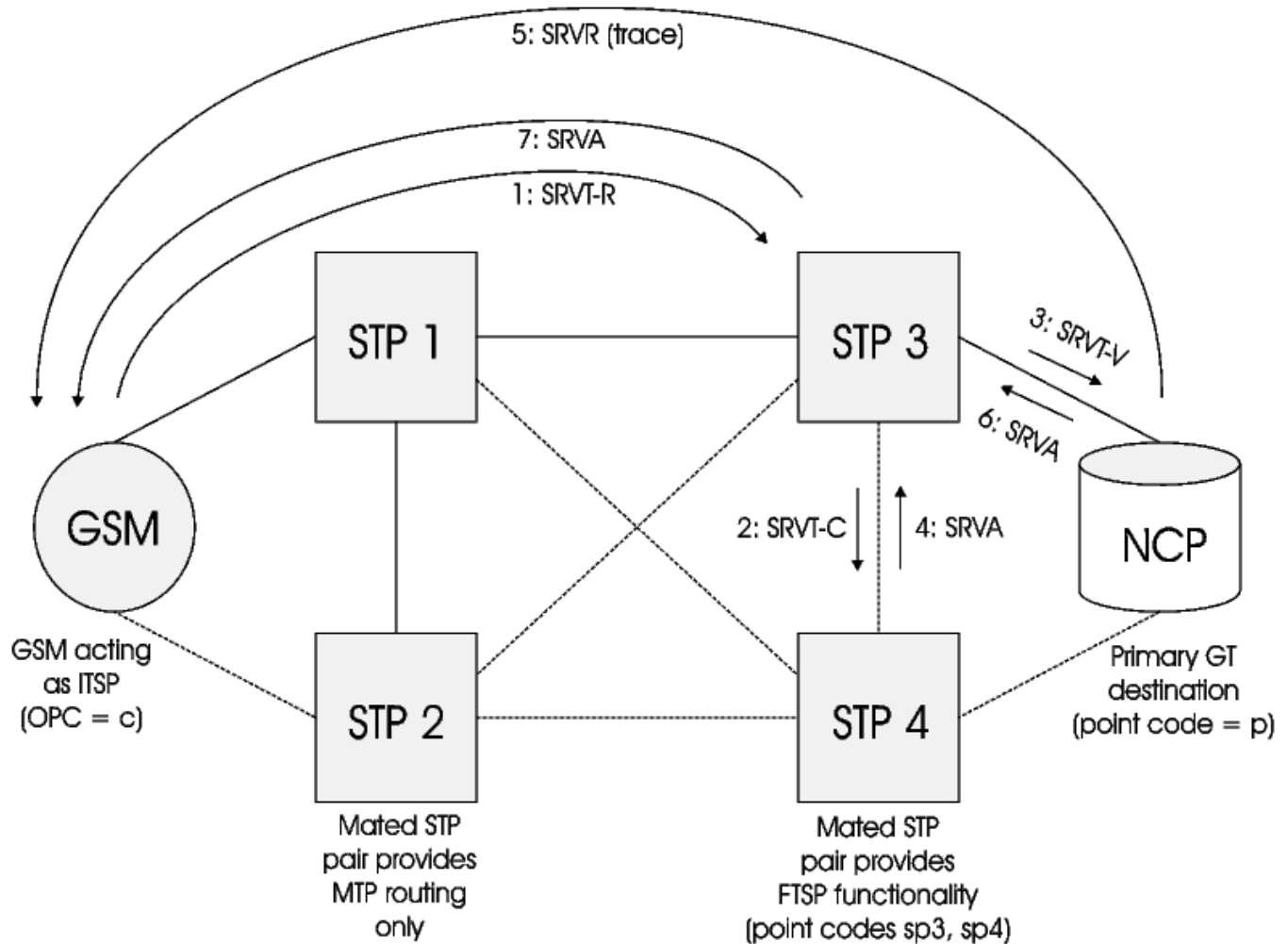


Figure 12.5-16 SRVT Example 2

The types of SRVT messages sent relate to the functionality provided at a specific signaling point. Message 1 is the *request* variant (SRVT-R) because the GSM is requesting further GTT analysis of the recipient TSP. Message 2 is the *compare* variant (SRVT-C), which compares GTT data in mated TSP pairs for consistency. Message 3 is the *verify* variant (SRVT-V), sent from a FTSP to a final GT destination, used to verify that the recipient signaling point can indeed process the target GT.

For this example, craft personnel issue the command:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c,TRACE
```

The output messages produced at the GSM for this test are:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST STARTED
TPC: sp3
MAX GTT ALLOWED: 2
TRACE REQUESTED
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS
SRVA RECEIVED FROM: sp3
SRVA RESULT: SUCCESS
```

```

EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS
TRACE SRVR FROM: p
NUMBER OF TSPS CROSSED: 3
TRACE LIST:
c sp3 sp4

EXC CCS SRVT TT=a DIGITS=b OPC=c TEST ENDED

```

The trace list includes the GSM's OPC (c) because it is providing TSP functionality. It also includes STP 3 (sp3), the TSP performing final GTT, as well as mate STP 4 (sp4), because its data has been compared for consistency. The default maximum number of GTTs allowed is 2, but a trace list containing 3 TSPs is *not* inconsistent; the maximum number allowed represents signaling points providing translations (which is two), while the trace list includes members of mated TSP pairs. See the EXCESSIVE LENGTH ROUTE entry in Table 12.5-3 for more details.

SRVT Example 3 illustrates a GSM that is provisioned to perform *remote GTT* processing: based upon translation type (TT=a) only (no digit analysis is performed), the GSM routes the message to a TSP for GTT processing. This is the most typical provisioning scenario for a GSM.

In this example, GTT processing is accomplished in two stages by two mated pairs of TSPs. The first pair of TSPs (STP 1 and STP 2) provides *intermediate GTT*, and that pair of STPs is known to the GSM by their *capability* (or *alias*) point code cc. The *final GTT* is performed by another pair of TSPs (STP 3 and STP 4), which yield both *primary* and *secondary* GT destinations (with point codes p and s, respectively). A trace is also requested by craft personnel. This network architecture is illustrated in Figure 12.5-17, with test message flows indicated.

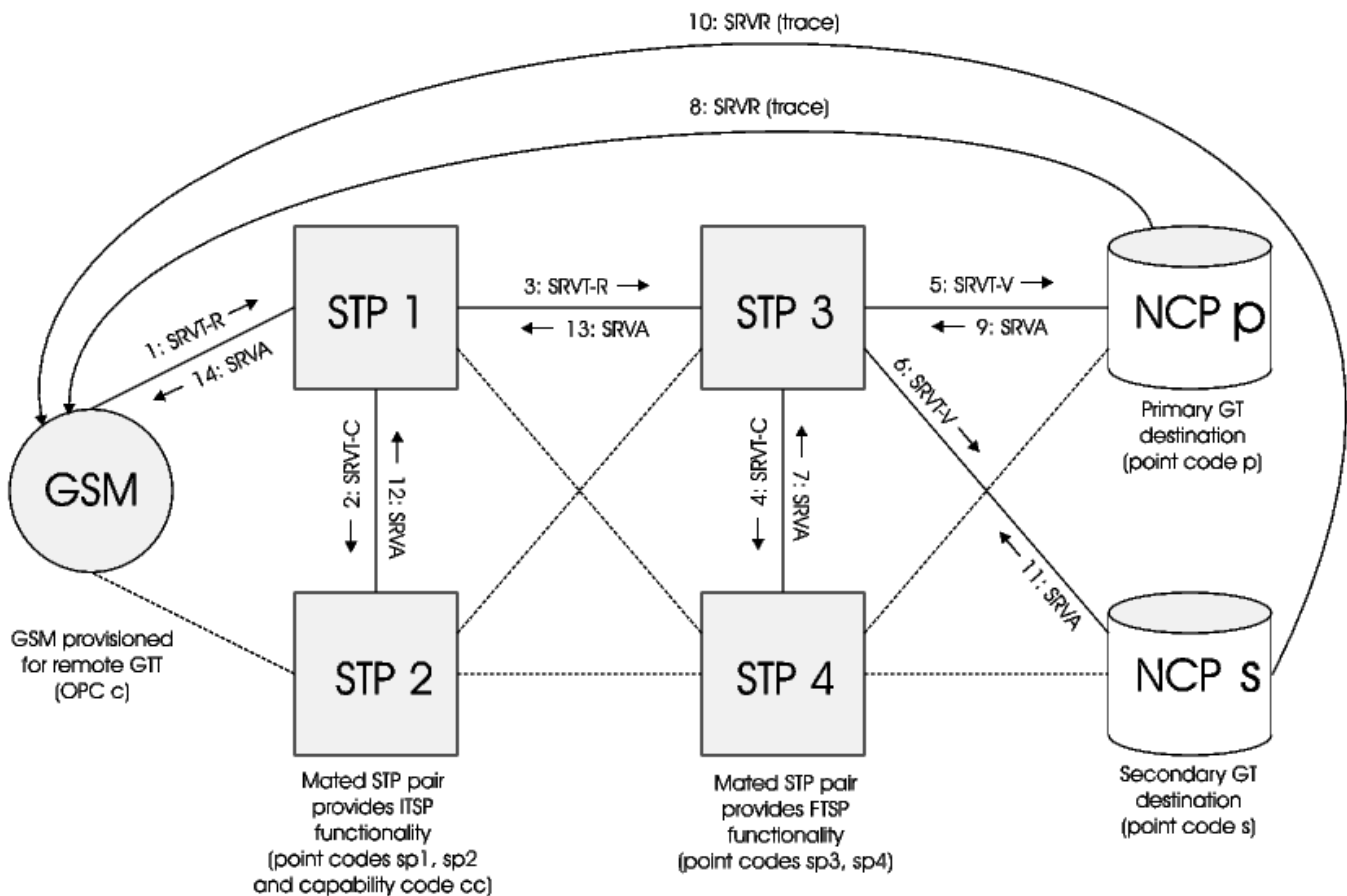


Figure 12.5-17 SRVT Example 3

The types of *SRVT* messages sent relate to the type of functionality provided by the receiving point code. Messages 1 and 3 are *request* variants (*SRVT-R*) because a request is being made of the receiving TSP to perform intermediate or final GTT. Messages 2 and 4 are *compare* variants (*SRVT-R*) that compare GTT data in mated TSP pairs. Messages 5 and 6 are *verify* variants (*SRVT-V*), sent to primary or secondary GT destinations to verify their ability to process the target GT.

The use of a *capability* (or *alias*) point code *cc* to represent the mated STP 1/STP 2 pair has no direct impact on *SRVT* functionality. A combined link set is provisioned to directly route to STP 1 or STP 2, and MTP routing distributes messages between the two STPs (in this example, the *SRVT-R* message is directed to STP 1 by the resident MTP routing algorithm). When either TSP in a mated pair receives a message addressed to the *capability code*, it treats that capability code as if its own point code is matched. Regardless of the member in a mated TSP pair that receives the message, the *compare SRVT-C* message ensures that the GTT data on both TSPs is consistent (for the GT under test).

For this example, craft personnel issue the command:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c,TRACE
```

The output messages produced at the GSM for this test are:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST STARTED
TPC: cc
MAX GTT ALLOWED: 2
TRACE REQUESTED
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS
SRVA RECEIVED FROM: sp1
SRVA RESULT: SUCCESS
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS
TRACE SRVR FROM: p
NUMBER OF TSPS CROSSED: 4
TRACE LIST:
sp1 sp2 sp3 sp4
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS
TRACE SRVR FROM: s
NUMBER OF TSPS CROSSED: 4
TRACE LIST:
sp1 sp2 sp3 sp4
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST ENDED
```

The initial TPC in the first output message is the capability code *cc* of a TSP pair. The *SRVA* returned, however, is from *sp1*, the member of the mated pair that receives the *SRVT-R* message from the GSM.

Traces are provided by both *primary* and *secondary* GT destinations (point codes *p* and *s*, respectively). The trace list does not include the GSM's OPC (*c*) because it is providing no TSP functionality. It also includes STP 1 (point code *sp1*) and STP 3 (*sp3*), the TSPs performing intermediate or final GTT, as well as mate STP 2 (*sp2*) and STP 4 (*sp4*), because their data is compared for consistency. The maximum number of GTTs allowed (two TSPs actually performing GTTs) is *not* exceeded because that count includes only the TSPs (*sp1* and *sp3*) that provide the translations to forward *SRVT* messages toward their GT destination.

For the final fault-free example (*SRVT Example 4*), consider a GSM that is provisioned for *remote GTT* processing,

and a *primary* and *backup* SCCP route destination that are provisioned to serve the target translation type (TT=a). The TSPs in this case are local non-mated STPs (point codes x and y), and GTT analysis at each TSP yields a single *primary* GT destination (point code p). A trace is also requested by craft personnel. This network architecture is illustrated in Figure 12.5-18, with test message flow indicated.

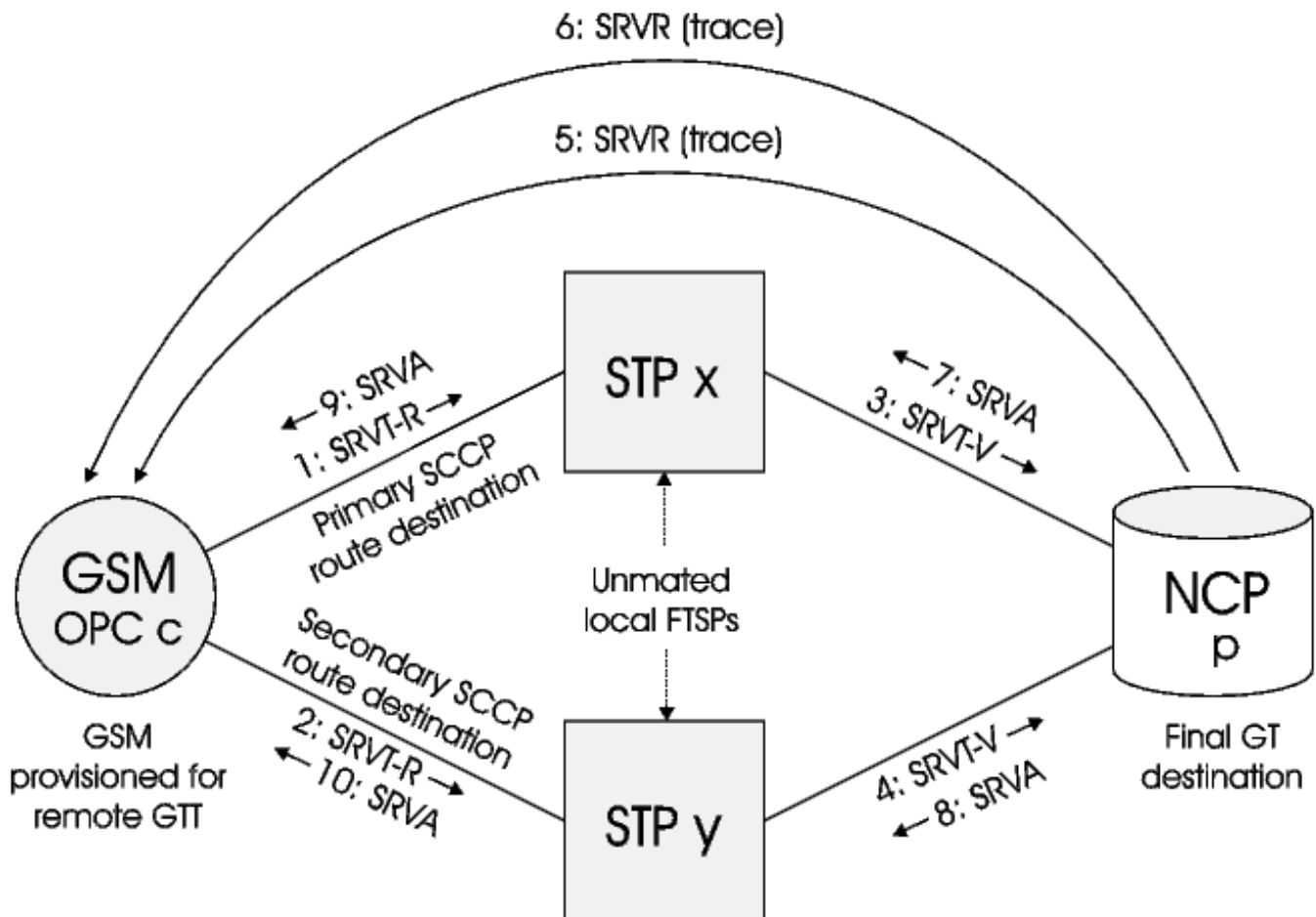


Figure 12.5-18 SRVT Example 4

For this example, craft personnel issue the command:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c,TRACE
```

The output messages produced at the GSM for this test are:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST STARTED
TPC: x, y
MAX GTT ALLOWED: 2
TRACE REQUESTED
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS
SRVA RECEIVED FROM: x
SRVA RESULT: SUCCESS
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS
SRVA RECEIVED FROM: y
```


SRVA RESULT: SUCCESS

EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS

TRACE SRVR FROM: p

NUMBER OF TSPS CROSSED: 1

TRACE LIST:

x

EXC CCS SRVT TT=a DIGITS=b OPC=c SUCCESS

TRACE SRVR FROM: p

NUMBER OF TSPS CROSSED: 1

TRACE LIST:

y

EXC CCS SRVT TT=a DIGITS=b OPC=c TEST ENDED

12.5.3.3.5 Partial Success or Failure SRVT Scenarios

This section presents SRVT scenarios in which one or more SCCP routing or GTT errors are detected during testing (the more interesting cases). Some of the possible SRVT error codes are not considered because of their similarity to examples presented for MRVT: LOOP, UNKNOWN INITIATING POINT CODE, EXCESSIVE LENGTH ROUTE, TIMER EXPIRED, and LOCAL CONDITIONS. More complex general examples (not GSM-specific) are presented in 256-015-300, *SS7 LEC Network Operations, Administration, and Maintenance*.

For SRVT Example 5, consider a GSM that is provisioned for *remote GTT* processing for a specific GT (TT=a, DIGITS=b). The *final GTT* should be handled by a mated TSP pair (STP 1 and STP 2, with capability code f), but the C-link between the TSP members is down (inaccessible route condition). Additionally, the GTT data in the FTSP under test is in error, routing an SRVT-V to an unrelated SEP (point code x) that is not the correct final GT destination. The network architecture for this example is illustrated in Figure 12.5-19, with message flow indicated (message numbers indicate the probable order of generation in time).

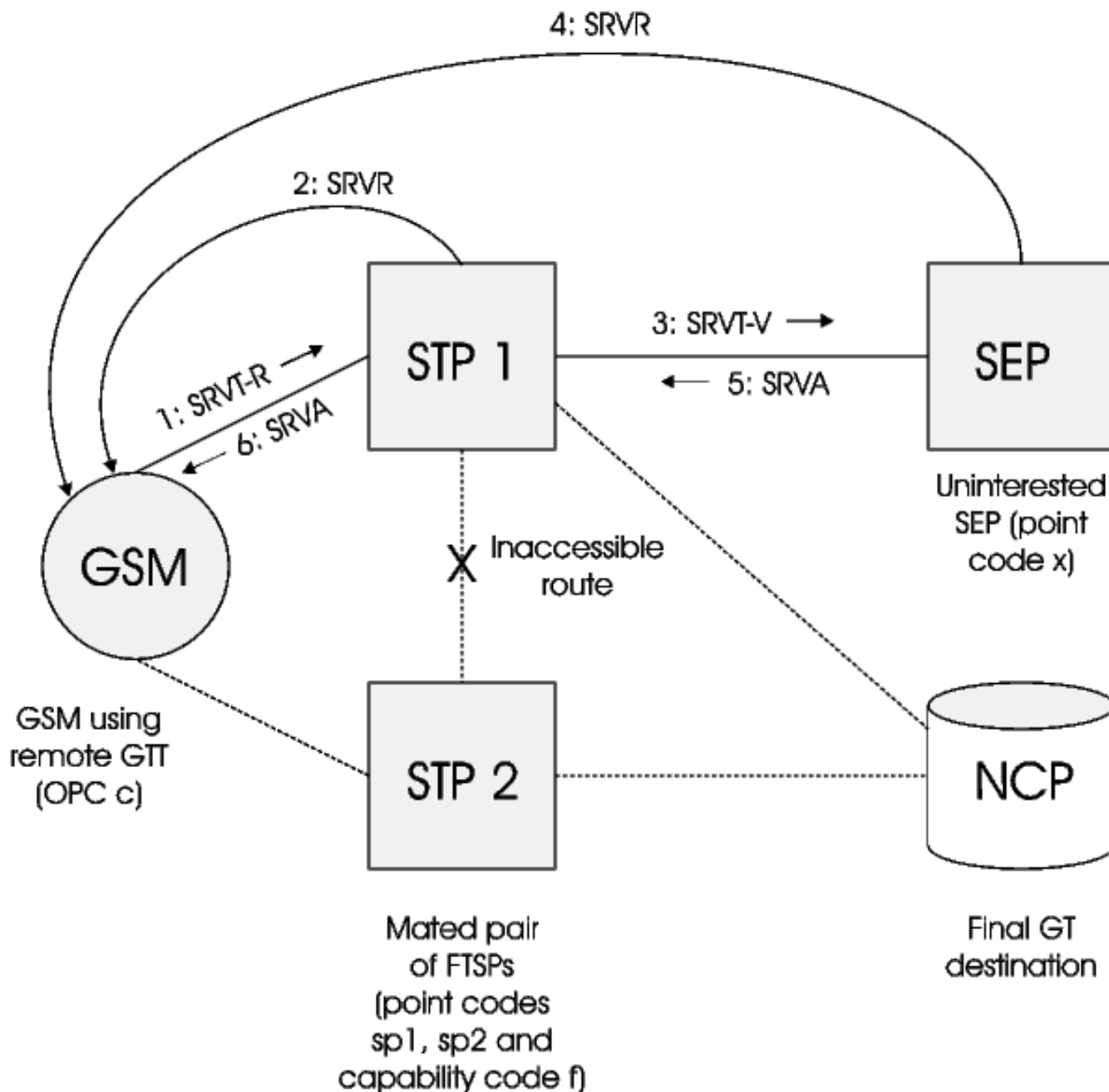


Figure 12.5-19 SRVT Example 5

For this example, craft personnel issue this command on the 5ESS®-2000 switch containing the target GSM:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c
```

The output messages produced by the GSM for this test are:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST STARTED
TPC: f
MAX GTT ALLOWED: 2
NO TRACE REQUESTED
```

```

EXC CCS SRVT TT=a DIGITS=b OPC=c FAILURE
SRVA RECEIVED FROM: sp1
SRVA RESULT: FAILURE
ERROR DETECTED:
WRONG SP
INACCESSIBLE ROUTE

```

```

EXC CCS SRVT TT=a DIGITS=b OPC=c FAILURE
SRVR RECEIVED FROM: sp1
ERROR DETECTED: INACCESSIBLE ROUTE
SUPPLEMENTAL INFO:
sp2

```

```

EXC CCS SRVT TT=a DIGITS=b OPC=c FAILURE
SRVR RECEIVED FROM: x
ERROR DETECTED: WRONG SP
SUPPLEMENTAL INFO:
sp1

```

```

EXC CCS SRVT TT=a DIGITS=b OPC=c TEST ENDED

```

The first `SRVR` indicates that an inaccessible SCCP route is detected by STP 1, and the mate STP 2 is inaccessible as noted by supplementary data `sp2`. The second `SRVR` indicates that the SEP (point code x) detected is not the correct final GT destination, which returns the `SRVR`; supplemental data `sp1` specifies the TSP that misrouted the `SRVT-V` message.

The flow of `SRVAs` starts with message 5, with the `WRONG SP` error encoded. At STP 1, the error in the received `SRVA` (message 5) is combined with the locally detected `INACCESSIBLE ROUTE` error (to its mate STP 2), both of which are returned to the initiating GSM in a single `SRVA` (message 6) and reported to craft personnel.

For `SRVT` Example 6, consider a GSM that performs *intermediate GTT* for the tested GT (`TT=a`, `DIGITS=b`). The GSM directs an `SRVT-R` message to a member of a mated TSP pair (STP 1/STP 2, with capability code f). The FTSP that receives the `SRVT-R` message (STP 1) has GTT data to determine the proper final GT destination (SEP with point code p), but the results of same translation on the mate STP 2 yield different results. The network architecture, as well as the message flow, is illustrated in Figure 12.5-20 .

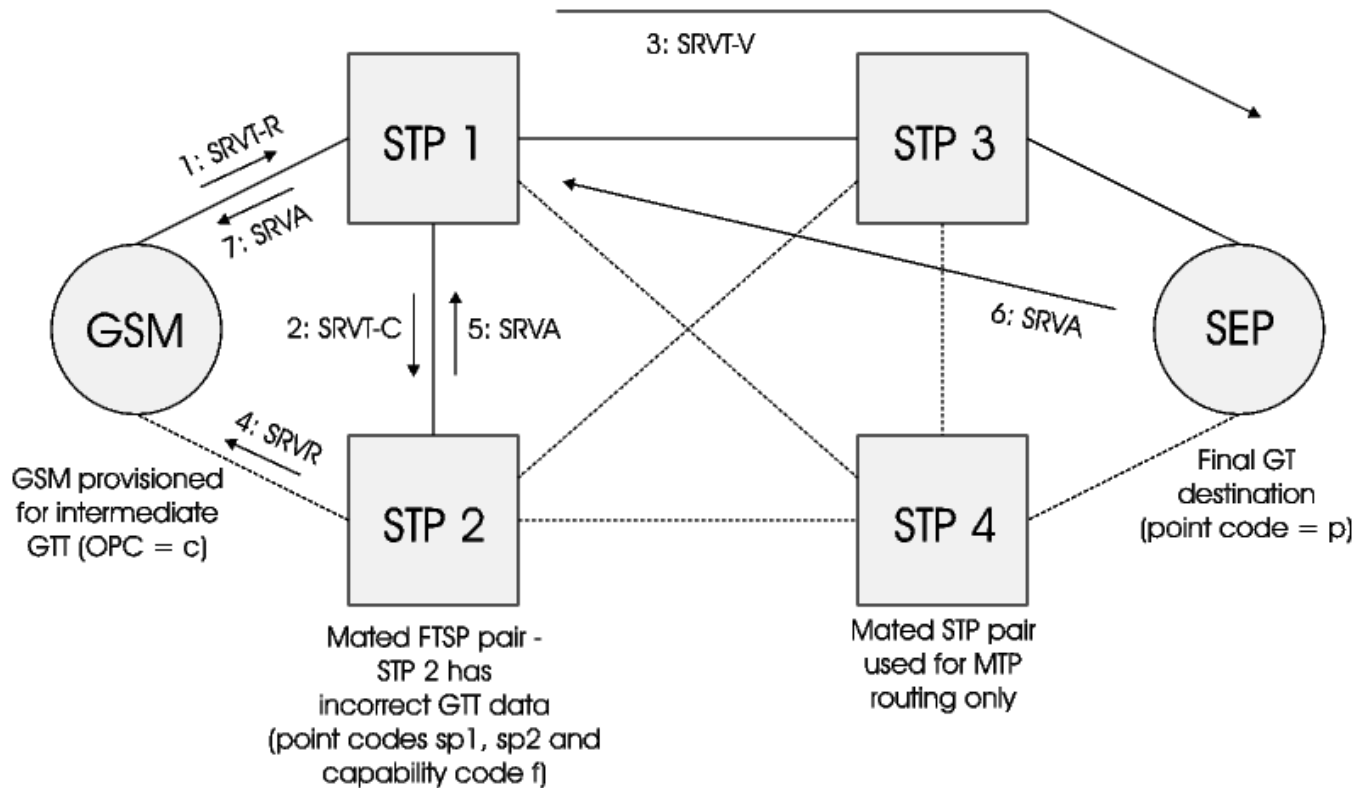


Figure 12.5-20 SRVT Example 6

For this example, craft personnel issue the input command:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c
```

These output messages are produced by the GSM:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST STARTED
TPC: f
MAX GTT ALLOWED: 2
NO TRACE REQUESTED
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c PARTIAL SUCCESS
SRVA RECEIVED FROM: sp1
SRVA RESULT: PARTIAL SUCCESS
ERRORS DETECTED:
INCORRECT TRANSLATION FOR PRIMARY DESTINATION
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c PARTIAL SUCCESS
SRVR RECEIVED FROM: sp2
ERROR DETECTED: INCORRECT TRANSLATION FOR PRIMARY DESTINATION
SUPPLEMENTAL INFO:
c sp1
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST ENDED
```

The SRVR in the output (because of 4: SRVR) reports the discrepancy in GTT data detected at STP 2, and the supplemental information provided specifies the mate TSP (STP 1 or point code sp1).

For SRVT Example 7, consider a GSM that performs *intermediate GTT* processing for the tested GT (TT=a, DIGITS=b). The GSM directs the message to an ITSP mated pair (STP 1 and STP 2 with capability code i), which in turn should route to a mated FTSP pair for *final GTT* processing. The ITSP member receiving the SRVT-R message has correct translation data to continue the test, but its mated TSP (STP 2) has erroneous GTT data. Also, the FTSP receiving the SRVT-R message has no translation data for the tested GT. See Figure 12.5-21 for this network architecture, and the test message flow.

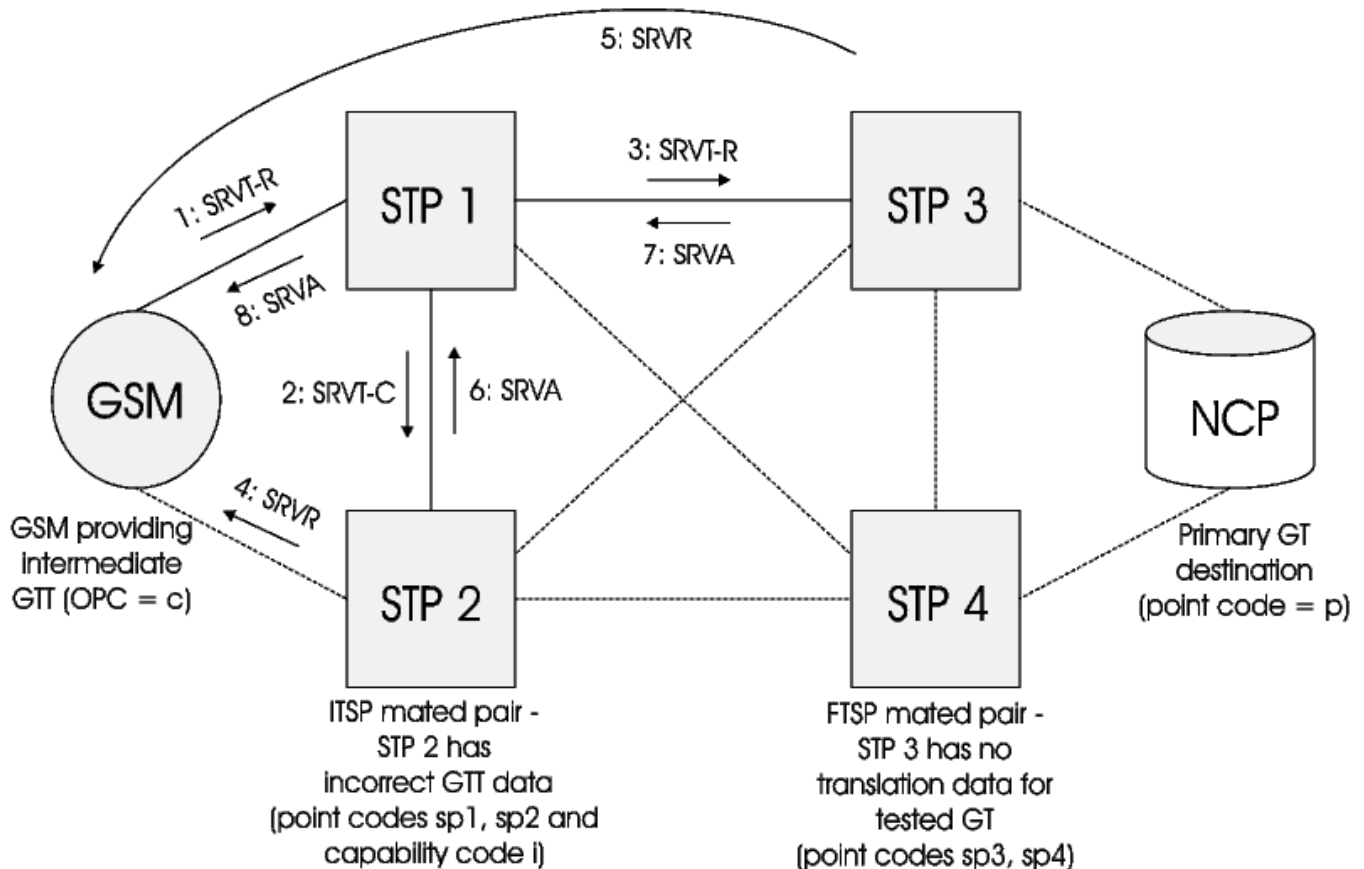


Figure 12.5-21 SRVT Example 7

For this example, craft personnel issue the input command (noting that three GTTs are allowed before reaching the final destination):

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c,NTSP=3
```

These output messages are produced by the GSM:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST STARTED
TPC: i
MAX GTT ALLOWED: 3
NO TRACE REQUESTED
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c FAILURE
SRVA RECEIVED FROM: sp1
SRVA RESULT: FAILURE
ERROR DETECTED:
INCORRECT TRANSLATION FOR INTERMEDIATE TSP
```

NO TRANSLATION FOR GLOBAL TITLE

```
EXC CCS SRVT TT=a DIGITS=b OPC=c FAILURE
SRVR RECEIVED FROM: sp2
ERROR DETECTED: INCORRECT TRANSLATION FOR INTERMEDIATE TSP
SUPPLEMENTAL INFO:
c sp1
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c FAILURE
SRVR RECEIVED FROM: sp3
ERROR DETECTED: NO TRANSLATION FOR GLOBAL TITLE
SUPPLEMENTAL INFO:
c sp1 sp2
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST ENDED
```

The first error `SRVR` in the output indicates a discrepancy in STP 1/STP 2 GTT data (the output message indicates sp2 detected the discrepancy, supplemental information indicates the mate TSP sp1).

The second `SRVR` message indicates that STP 3 (sp3) has no ability to translate the tested GT, and supplemental information provides the trace of TSPs crossed leading to the `SRVT-R` message sent (STP 1 or sp1 sent the message, sp2 is the mate added to the trace list by the compare function).

For the final example (SRVT Example 8), consider a GSM that is provisioned for *remote GTT* processing for a specific translation type (TT=a). The GSM directs messages to a mated ITSP pair (STP 1/STP 2 with capability code i), which in turn routes to a mated FTSP pair (STP 3/STP 4). The initial routing from the GSM is to STP 1, which performs proper intermediate GTT and routes an `SRVT` message to STP 3; the mate of the ITSP pair (STP 2) has identical translation data. STP 3 and its mate STP 4 have appropriate translation data to perform a final GTT to a *primary* and *secondary* mated pair of SCP final GT destinations (point codes p and s, respectively), but STP 3 has no SCCP routing data to reach the *primary* GT destination. Data on the secondary GT destination has no knowledge the tested GT that it should process. The network architecture, as well as message flows, for this error-ridden example is illustrated in Figure 12.5-22 .

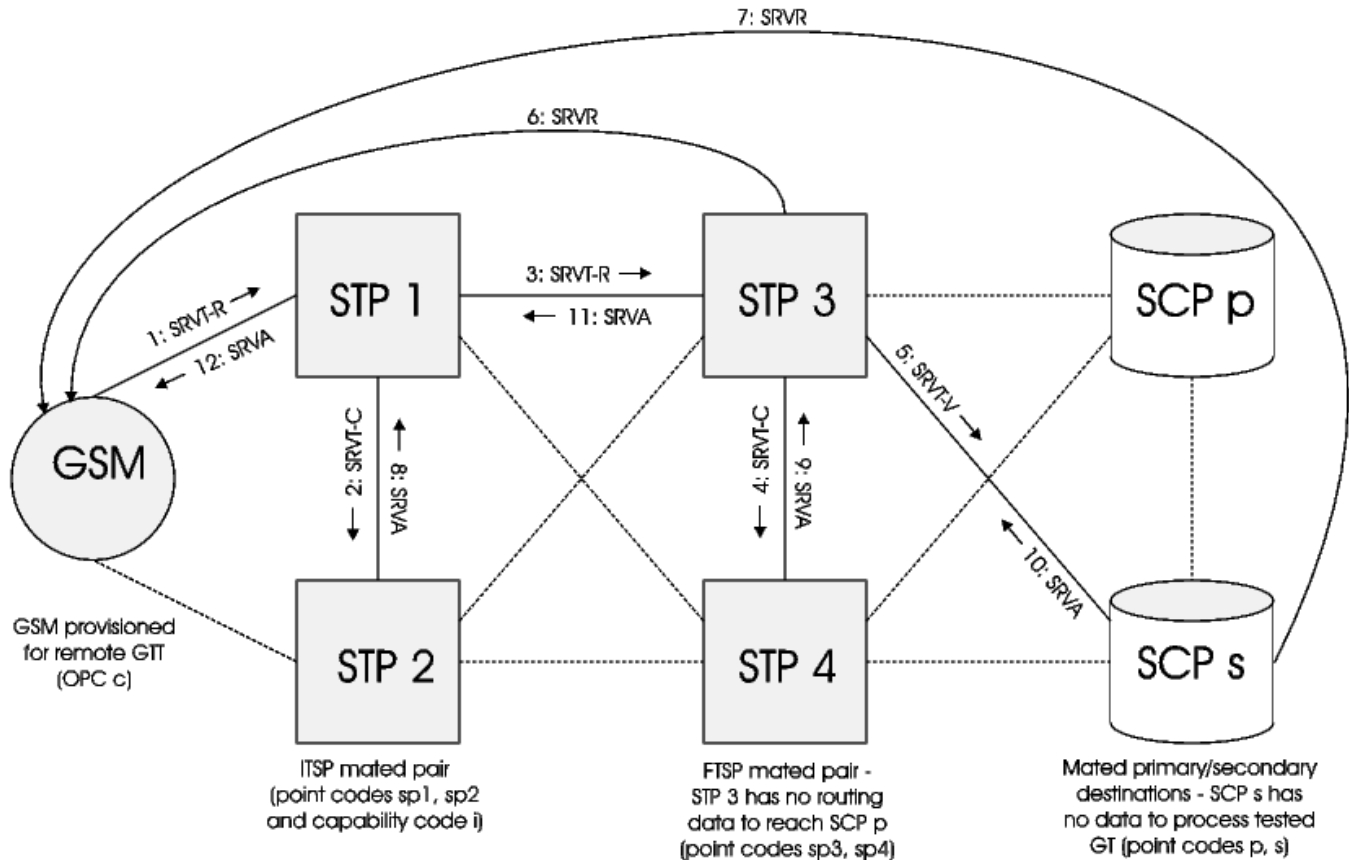


Figure 12.5-22 SRVT Example 8

For this example, craft personnel issue the input command:

```
EXC:CCS,SRVT,TT=a,DIGITS=b,OPC=c
```

These output messages are produced from the GSM:

```
EXC CCS SRVT TT=a DIGITS=b OPC=c TEST STARTED
TPC: i
MAX GTT ALLOWED: 2
NO TRACE REQUESTED

EXC CCS SRVT TT=a DIGITS=b OPC=c PARTIAL SUCCESS
SRVA RECEIVED FROM: sp1
SRVA RESULT: PARTIAL SUCCESS
ERRORS DETECTED:
ROUTING PROBLEM
NOT SECONDARY DESTINATION

EXC CCS SRVT TT=a DIGITS=b OPC=c PARTIAL SUCCESS
SRVR RECEIVED FROM: sp3
ERROR DETECTED: ROUTING PROBLEM
SUPPLEMENTAL INFO:
sp1 sp2
```

```
EXC CCS SRVT TT=a DIGITS=b OPC=c PARTIAL SUCCESS
SRVR RECEIVED FROM: s
ERROR DETECTED: NOT SECONDARY DESTINATION
SUPPLEMENTAL INFO:
sp1 sp2 sp3 sp4

EXC CCS SRVT TT=a DIGITS=b OPC=c TEST ENDED
```

The routing problem in the first `SRVR` is identified on STP 3 (point code `sp3`), with the primary GT destination not populated in SCCP routing. The inability to provide the requested translation for the tested GT (as cited in the second `SRVR` in the output) is detected on the secondary GT destination (point code `s`). The supplemental information in both cases is the trace list leading to the signaling point detecting the errors.

13. SS7 - PSU FEATURE IMPLEMENTATION

Procedure 13.1: SIGNALING LINK PROVISIONING

OVERVIEW

This section describes the provisioning required to define, modify or delete CCS signaling capabilities on an existing 5ESS®-2000 switch VCDX or 5ESS®-2000 switch GSM. Specific provisioning procedures are described in the subsections that follow this overview.

The procedures do not contain information about the selection of values to be negotiated with regional CCS management (such as trunk types, origination point codes, or destination point codes), and they do not describe information that is dependent on local office equipment, such as actual PSU termination assignments or DFI/DNU-S access assignments.

Each procedure contains "precheck" steps to ensure the success of the RC/V transactions. These prechecks minimize the need to investigate RC/V failures. See Table 13.1-1 for a list of the RC/V views used to provision this feature.

All of the procedures require access to RC/V views. Access is accomplished by choosing **196** on the menu selection, or the input message `rcv:menu:apprc` on an MCC/STLWS. Use the input message `apprc` on a UNIX®/RC terminal.

Some of the procedures that follow require specific **office records** be interrogated. In those procedures, an input command of the form

`OP:OFR, FORM=###, DEVICE=xxx`

will be specified. If **xxx** is "FILE", the office records will be deposited in a file `/rclog/OFR.Oy`, where **y** is the **REQUEST ID** in the command response; the file can be interrogated or printed according to local procedures. Alternately, if **xxx** is specified as "ttyR", output is produced directly on the resident office records printer (if available); other output destinations are possible, as defined on the `OP-OFR` input manual page in 235-600-700, *Input Messages Manual*.

See 235-118-2xx, *Recent Change Reference* and 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)* for detailed descriptions of RC/V fields.

Table 13.1-1 GSM Signaling RC/V Views

VIEW	TITLE	USE ^a	PURPOSE
7.41	TI CHANNEL USAGE	r	Review T1 channel usage on a DFI facility
7.42	DS1 CHANNEL USAGE	r	Review DS1 channel usage on a DNU-S facility
8.15	CCS OFFICE PARAMETERS	ru	Enable specific CCS features
16.1	GLOBAL SM	rid	Define GSM/OPC for VCDX or 5ESS®-2000 switch SM/SM-2000
16.2	LEVEL 3 TIMER PARAMETERS	ru	Update MTP Level 3 parameters
16.3	DATA LINK RATE TIMER PARAMETERS	ru	Update MTP Level 2 parameters
16.4	OMAP ROUTE VERIFICATION TEST TIMER PARAMETERS	u	Update OMAP parameters
16.5	SIGNALING LINK SET	riud	Add/update/delete GSM LSs
16.6	SIGNALING LINK SET MEMBER	riud	Add/update/delete GSM LS members
16.7	COMBINED SIGNALING LINK SET	riud	Define/update/delete GSM CLS
16.10	SIGNALING POINT CODE	riud	Define/update/delete GSM DPC
16.11	CHANNEL GROUP ASSIGNMENT DEFINITION	r	GSM CCS channel group member assignments
16.17	MESSAGE DELIVERY LINK	rid	Define/delete intra-SM MD link
16.20	SCCP NETWORKS DEFINITION	r	Check SCCP GSM definition
22.2	PACKET SWITCH UNIT	ru	Adjust PH3 or PH22 spares on PSU shelf 0

			and reserve PIDB timeslots ^b
22.3	PACKET SWITCH UNIT SHELF	ru	Adjust PH3 or PH22 spares on PSU shelves 1-4 ^b
22.16	PSU PROTOCOL HANDLER CHANNEL GROUP ASSIGNMENTS	ru	Define PH3 or PH22 channel group for CCS use ^b
Notes: a. The USE column indicates how the view is used: r - REVIEW i - INSERT u - UPDATE d - DELETE b. Prior to 5E14, only PH3 hardware can be provisioned for CCS use. In 5E14 and later software releases, PH22 hardware can also be used.			

To convert a 5ESS®-2000 switch VCDX or 5ESS®-2000 switch SM/SM-2000 (without CCS functions) to a GSM with a PSU platform for CCS signaling access, use the procedures shown in Table 13.1-2. The individual procedures are self contained, but should be performed in the sequence listed.

Table 13.1-2 SM/SM-2000 to GSM Conversion

JOB DESCRIPTION	PROCEDURE
Convert to a CCS GSM	Procedure 13.1.1
Reset exchange MTP Level 2 parameters	Procedure 13.1.2
Reset exchange MTP Level 3 parameters	Procedure 13.1.3
Define intra-SM MD link	Procedure 13.1.4
Define new LSs	Procedure 13.1.5
Define new CLSs	Procedure 13.1.6
Define new DPCs	Procedure 13.1.7
Prepare PSU for CCS assignments	Procedure 13.1.8
Define new link set members (CCSLKs)	Procedure 13.1.10
Update 5E13 enhanced features	Procedure 13.1.21
Update OMAP parameters	Procedure 13.1.22

Once a GSM is established, many of the same procedures are used to change signaling routes, change link set composition, or change signaling link termination/access characteristics. See Table 13.1-3 for a list of provisioning activities to use as needed.

Table 13.1-3 On-going GSM SS7 Provisioning Activities

JOB DESCRIPTION	PROCEDURE
Convert PH3 to PH22	Procedure 13.1.9
Reset exchange MTP Level 2 parameters	Procedure 13.1.2
Reset exchange MTP Level 3 parameters	Procedure 13.1.3
Redefine intra-SM MD link termination	Procedure 13.1.11
Define new LSs	Procedure 13.1.5
Delete obsolete LSs	Procedure 13.1.18
Define new CLS	Procedure 13.1.6
Redefine CLS members	Procedure 13.1.12
Delete obsolete CLS	Procedure 13.1.17
Define new DPCs	Procedure 13.1.7
Modify CLS/LSs serving DPCs	Procedure 13.1.13
Delete obsolete DPCs	Procedure 13.1.16
Define new LS members	Procedure 13.1.10
Modify CCSLK characteristics	Procedure 13.1.14
Delete obsolete LS members	Procedure 13.1.15
Update 5E13 enhanced features	Procedure 13.1.21
Update OMAP parameters	Procedure 13.1.22

To delete CCS functionality from a GSM use the procedures shown in Table 13.1-4 .

Table 13.1-4 Removal of CCS Capabilities from a GSM

JOB DESCRIPTION	PROCEDURE
Delete all LS members	Procedure 13.1.15
Delete all DPCs	Procedure 13.1.16
Delete CLSs	Procedure 13.1.17
Delete all LSs	Procedure 13.1.18
Delete intra-SM MD link	Procedure 13.1.19
Undefine GSM existence	Procedure 13.1.20

The signaling link provisioning procedures in this section are:

PROCEDURE

1. Procedure 13.1.1 - Convert to a CCS Global Switching Module
2. Procedure 13.1.2 - Reset Exchange MTP Level 2 Parameters
3. Procedure 13.1.3 - Reset Exchange MTP Level 3 Parameters
4. Procedure 13.1.4 - Define Intra-SM Message Delivery Link
5. Procedure 13.1.5 - Define New Link Sets
6. Procedure 13.1.6 - Define a New Combined Link Set
7. Procedure 13.1.7 - Define New Destination Point Codes
8. Procedure 13.1.8 - Preparing the Packet Switch Unit for CCS Assignment
9. Procedure 13.1.9 - Convert PH3 to PH22 Hardware
10. Procedure 13.1.10 - Define New Link Set Members
11. Procedure 13.1.11 - Redefine Intra-SM Message Delivery Link Termination
12. Procedure 13.1.12 - Redefine Combined Link Set Members
13. Procedure 13.1.13 - Modify Link Sets Serving a DPC
14. Procedure 13.1.14 - Modify Link Member Characteristics
15. Procedure 13.1.15 - Delete Link Set Members
16. Procedure 13.1.16 - Delete Destination Point Codes
17. Procedure 13.1.17 - Delete Combined Link Sets
18. Procedure 13.1.18 - Delete Link Sets
19. Procedure 13.1.19 - Delete Intra-SM Message Delivery Link
20. Procedure 13.1.20 - Undefine CCS Global Switching Module Existence
21. Procedure 13.1.21 - Provisioning of 5E13 Maintenance Enhancements

22. Procedure 13.1.22 - Operation, Maintenance and Administration Part Provisioning

Procedure 13.1.1: Convert to a CCS Global Switching Module

OVERVIEW

Before any signaling routes (including link sets/members or destination point codes) can be defined for CCS access through a PSU platform, the SM/SM-2000 must be provisioned as a global switching module (GSM) in the office dependent data (ODD). This procedure accomplishes the definition.

The origination point code (OPC) to be assigned to the GSM should be negotiated with regional CCS management before starting this procedure.

PROCEDURE

1. First determine if the target SM/SM-2000 has the appropriate software configuration to support CCS functionality on a PSU.

At an RC/V terminal, enter **18.1r** to access the SWITCHING MODULE view in REVIEW mode. Specify the key field:

SM	(proposed GSM number)

and observe the CONFIGURATION field on screen 4.

- If the configuration specified is **SIGNALING** or **SM2000** (which will support CCS functionality on a PSU), CONTINUE this procedure.
- Otherwise, EXIT the procedure immediately. Choose another SM/SM-2000 as a GSM candidate, or convert the SM's software configuration according to local practices, and then RESTART this procedure.

Enter < to return to the forms menu and **q** to exit RC/V.

2. Check to see if the target SM/SM-2000 is equipped with a packet switch unit (PSU). A PSU must be equipped in order to provide signaling link terminations on a GSM. Attempt to display the **PACKET SWITCH UNIT** page on an MCC/STLWS, using the command **1186,xxx**, where **xxx** is the target SM/SM-2000.

- If the 1186 MCC page is not displayed, a PSU is not equipped on the target SM/SM-2000; EXIT this procedure immediately.

See 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures-Growth* for procedures to grow a PSU on the SM/SM-2000, and, once completed, RESTART this procedure.

- If the 1186 MCC page is displayed, the PSU is equipped (status/shelf equipage is irrelevant at this point), so CONTINUE this procedure.

3. Determine if the SM/SM-2000 is already defined as a GSM by issuing the input message:

OP: CCS, GSM, SM=xxx

on an MCC/STLWS, where **xxx** is the target SM/SM-2000 number.

- If the request succeeds, the target SM/SM-2000 has already been defined as a GSM and this procedure

is not appropriate; EXIT this procedure immediately.

- If the request fails (response "NG - GSM MISMATCH" or "NG - NO GLOBAL SM IN OFFICE"), the target SM/SM-2000 has not yet been defined as a GSM; CONTINUE this procedure.

- At an RC/V terminal, enter **16.1i** to access the GLOBAL SM view in INSERT mode.

Enter the following data for the new GSM:

GSM	(target SM/SM-2000 number)
OPC	(enter 9-digit OPC associated with the new GSM)
CONGEST METHOD	(enter TIMER or RCT congestion method)

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

- Enter **i** to complete the insert.

- If the insertion completes successfully, "FORM INSERTED" flashes in the upper right corner of the screen. Enter **<** to return to the forms menu and **q** to quit recent change.

Before continuing, monitor the ROP for messages indicating the success of the allocation of an optional data region (ODR) for the GSM's pumpable incoming routing data (target image ICR); be patient, as response is highly dependent on SM occupancy. After the output messages

```
CFR SPRMEM IMAGE=ICR SM=xxx TYPE=GROW COMPLETED
CFR SPRMEM IMAGE=SPAREMEM SM=xxx TYPE=GROW COMPLETED
MEMORY POINTERS UPDATED - ODD BACKUP REQUIRED
```

appear in the 5E11 software release (where **xxx** is the target GSM), the allocation of the ICR image was successful. This process may have "stolen" current stand-alone billing memory (SABM) to accomplish the allocation. The current size of SABM should be verified and possibly be grown according to local practices; refer to *5ESS®-2000 Switch Engineering Information, Index 11* for guidance.

In 5E12 and later software releases, a slightly different output appears:

```
CFR SPRMEM ODRID=ICR SM=xxx TYPE=GROW COMPLETED
CFR SPRMEM ODRID=SPAREMEM SM=xxx TYPE=GROW COMPLETED
MEMORY POINTERS UPDATED - ODD BACKUP REQUIRED
```

As allocation of ODRs in 5E12 and later software releases use *only SPARE MEMORY*, the size of the SABM region has *not* changed.

SKIP to Step 7.

- Otherwise, the attempted provisioning has failed. Enter **<** to return to the forms menu and **q** to quit recent change, and CONTINUE this procedure.

- Monitor the ROP for messages indicating the failure of the allocation of an ODR for the ICR image. Follow the instructions, based upon the nature of the message produced:

- The following output message

```
CFR SPRMEM IMAGE=ICR SM=xxx TYPE=GROW FAILED
SABM SHRINKAGE FAILURE
```

could appear in the 5E11 software release, where **xxx** is the target GSM.

This message indicates an attempt to shrink SABM to provide enough spare memory for ODR allocation has failed, as the SABM region contains active records. Exit this procedure now, and reenter later after billing records have been offloaded.

— The following output message

```
CFR SPRMEM IMAGE=ICR SM=xxx TYPE=GROW FAILED
INSUFFICIENT SPARE SM MEMORY
```

could appear in the 5E11 software release, where **xxx** is the target GSM.

In this case, ODR growth cannot be accomplished (even if SABM in excess of the required minimum is converted to spare memory) and new physical memory must be grown. Use *PROCEDURE 3.27, Perform SM Memory Growth Procedure* in the 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures - Growth* document, and then reenter this procedure.

— The output message

```
CFR SPRMEM ODRID=ICR SM=xxx TYPE=GROW FAILED
INSUFFICIENT SPARE SM MEMORY
```

could appear in 5E12 and later software releases, where **xxx** is the target GSM.

In these software releases, a failure in the allocation of an ODR for a target ICR image indicates only that sufficient SPARE MEMORY is not available, but engineerable memory regions for SABM or real-time billing memory (RTBM) can be reduced according to local practices, rather than growing in new physical memory.

In addition to the above failure indication, additional data will indicate the size of the desired ICR image, the size of current spare memory, the sizes of current SABM and RTBM regions (if provisioned), as well as the amount of SABM/RTBM memory that can be reconfigured into spare memory which can be used for ODR allocation. If the sum of spare memory, plus the configurable segment of SABM/RTBM memory is sufficient to allocate the ICR image, appropriate SABM/RTBM degrowth can be considered. If according to local practices, sufficient degrowth of SABM/RTBM regions can be accomplished, this procedure should be reentered. See *5ESS®-2000 Switch Engineering Information, Index 8* for guidance in degrowing the SABM region, and 235-200-110, *5ESS®-2000 Switch Long Distance Platform Document* for guidance in degrowing the RTBM region.

If sufficient degrowth of SABM/RTBM regions is not possible, new physical memory must be grown. Use *PROCEDURE 3.27, Perform SM Memory Growth Procedure* in the 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures - Growth* document, and then reenter this procedure.

7. Display the **1532,xxx CCS LINK SET SUMMARY** page on an MCC/STLWS, where **xxx** is the new GSM number. The page is displayed, but no LSs (link sets) are identified.

8. Back up the new ODD by entering the input message:

```
BKUP:ODD
```

on an MCC/STLWS.

9. To prepare for further provisioning, the new image to be pumped into PH3s supporting CCS functionality must be downloaded in the GSM. To accomplish this, execute *PROCEDURE 3.95, Perform Protocol Handler*

(PH) Growth procedure in the 235-105-231, 5ESS®-2000 Switch Hardware Change Procedures - Growth document.

10. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.2: Reset Exchange MTP Level 2 Parameters

OVERVIEW

The message transfer part (MTP) Level 2 exchange timer parameters must be defined in the office dependent data (ODD). Default Level 2 timer parameters, for both 56 Kbps and 64 Kbps signaling links, have been installed in the SM/SM-2000 as the GSM was provisioned, but local exchange requirements may require adjustment. This procedure updates those parameters.

Before starting this procedure obtain the new timer values (see Table 13.1.2-1).

PROCEDURE

1. Determine if the target SM/SM-2000 is already defined as a global SM (GSM), by issuing the input message:

OP : CCS , GSM , SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM number.

- If the request fails (response "NG - GSM MISMATCH" or "NG - NO GLOBAL SM IN OFFICE"), the target SM/SM-2000 has not yet been defined as a GSM; EXIT this procedure immediately.

Use the procedure "Convert to a CCS Global Switching Module," Procedure 13.1.1 , to provision the GSM, and then RESTART this procedure.

- If GSM status is produced, the GSM has already been defined and this procedure is appropriate; CONTINUE this procedure.

2. Obtain the new Level 2 timer values from the exchange records, prior to beginning the RC/V activities. The Level 2 timer fields are listed in Table 13.1.2-1 with their allowed ranges/default values. For detailed descriptions of these timers see 235-118-2xx, *5ESS®-2000 Switch Recent Change Reference* or 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)*.

Table 13.1.2-1 MTP Level 2 Timer Range

TIMER FIELD	RANGE (milliseconds)	DEFAULT (milliseconds)
ALIGNED READY	13000-300000	13000
NOT ALIGNED	5000-150000	11500
ALIGNED	125-50000	11500
EMERG PROVING	400-3000	600
NORM PROVING	2300-9500	2300
SENDING SIB	80-250	100
REMOTE CONGESTION	3000-10000	3000
EXCESS DELAY ACK	500-2000	500

3. At an RC/V terminal, enter **16.3u** to access the DATA LINK RATE TIMER PARAMETERS view in UPDATE mode.

Specify the key fields:

GSM	(target GSM number)
DATA LINK RATE	(either 56KB or 64KB)

All the other fields listed in Table 13.1.2-1 are populated with current values and the string *Enter Update, Change, Validate, or Print*: is produced.

4. Enter **c** to start change mode. Enter the **number of the field** to be updated to move the cursor to that field. Enter the **new timer value**.

Continue entering new field numbers and timer values until all identified fields are changed.

5. Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

6. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

7. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.3: Reset Exchange MTP Level 3 Parameters

OVERVIEW

The message transfer part (MTP) Level 3 exchange timer parameters must be defined in office dependent data (ODD). Default Level 3 timer parameters have been installed in the SM/SM-2000 environment as the GSM was provisioned, but local exchange requirements may require adjustment. This procedure updates these parameters.

Before starting this procedure, obtain the new timer values (see Tables 13.1.3-1 and 13.1.3-2).

PROCEDURE

1. Determine if the target SM/SM-2000 is already defined as a global SM (GSM) by issuing the input message:

OP : CCS , GSM , SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM number.

- If the request fails (response "NG - GSM MISMATCH" or "NG - NO GLOBAL SM IN OFFICE"), the target SM/SM-2000 has not yet been defined as a GSM; EXIT this procedure immediately.

Use the procedure "Convert to a CCS Global Switching Module," Procedure 13.1.1, to provision the GSM, and then RESTART this procedure.

- If the request succeeds, the GSM has already been defined, and this procedure is appropriate; CONTINUE this procedure.

2. Obtain the new Level 3 timer values from the exchange records, prior to beginning the RC/V activities. The Level 3 timer fields are listed in Table 13.1.3-1 with their allowed ranges/default values. For detailed descriptions of these timers see 235-118-2xx, *5ESS®-2000 Switch Recent Change Reference* or 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)*.

Table 13.1.3-1 Pre-5E13 MTP Level 3 Timer Ranges

TIMER/PARAMETER	RANGE	DEFAULT
LINK AFFECT	1-6	2
CONGESTION	6-10	8
CO DELAY	500-1200 (ms)	500 (ms)
CO ACK	700-2000 (ms)	700 (ms)
CB DELAY	500-1200 (ms)	500 (ms)
CB ACK1	500-1200 (ms)	500 (ms)
CB ACK2	500-1200 (ms)	500 (ms)
CCR DELAY	500-1200 (ms)	500 (ms)
TRANSFER	800-1200 (ms)	1000 (ms)
SRT WAIT	30000-60000 (ms)	30000 (ms)
UA WAIT	800-1500 (ms)	1000 (ms)
MSU WAIT	800-1500 (ms)	1000 (ms)
INHIBIT ACK	2000-3000 (ms)	3000 (ms)
RSC TEST	2000-3000 (ms)	3000 (ms)
RSC UPDATE	1400-2000 (ms)	1400 (ms)
LINK RESTART	800-1500 (ms)	1000 (ms)
LOCAL INHIBIT	90000-120000 (ms)	120000 (ms)
REMOTE INHIBIT	90000-120000 (ms)	120000 (ms)
STOP SEND WAIT	800-1200 (ms)	1000 (ms)
SLS WAIT	800-1200 (ms)	1000 (ms)
BSNT WAIT	160-240 (ms)	200 (ms)
LEVEL 2 WAIT	240-360 (ms)	300 (ms)
RC TIME	2000-24000 (ms)	8000 (ms)

SMH WAIT	780000-1020000 (ms)	900000 (ms)
ACK LINK TEST	4000-12000 (ms)	4000 (ms)
DELAY LINK TEST	30000-90000 (ms)	90000 (ms)

In 5E13 and later software releases, new timers associated with detection of false link congestion and production of link alignment failure reports are available (as noted in Table 13.1.3-2).

Table 13.1.3-2 5E13 and Later MTP Level 3 Timer Ranges

TIMER	RANGE	DEFAULT
FALSE LINK CONG	10-120 (sec)	30 (sec)
FAILED LINK REF	180-600 (sec)	480 (sec)

- At an RC/V terminal, enter **16.2u** to access the LEVEL 3 TIMER PARAMETERS view in UPDATE mode.
- Enter the appropriate **GSM** key field (the target GSM number). All the other fields listed in pre-5E13 Table 13.1.3-1 and 5E13 and later Table 13.1.3-2 are populated with current values, and the string *Enter Update, Change, Validate, or Print:* is produced.
- Enter **c** to start change mode. The expected response is *Change field:* string. Enter the **number of the field** to be updated to move the cursor to that field. Enter the **new timer value**.

Continue entering new field numbers and timer values until all identified fields are changed.

- Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

- Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

- STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.4: Define Intra-SM Message Delivery Link

OVERVIEW

The intra-SM message delivery (MD) link is critical to the operation of CCS activities on a PSU platform. This procedure can be used to install the intra-SM MD link into a new GSM, or as an integral part of a procedure to change the PSU channel group termination of an existing intra-SM MD link.

The PH channel group assignment should be known before entering this procedure.

PROCEDURE

1. Determine if the target SM/SM-2000 is defined as a GSM by issuing the input message:

OP : CCS , GSM , SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM number.

- If the request fails (response "NG - GSM MISMATCH" or "NG - NO GLOBAL SM IN OFFICE"), the target SM/SM-2000 has not yet been defined as a GSM; EXIT this procedure immediately.

Use the procedure "Convert to a CCS Global Switching Module," Procedure 13.1.1, to provision the GSM, and then RESTART this procedure.

- If the request succeeds, the GSM has already been defined, and this procedure is appropriate; CONTINUE this procedure.

2. Is this the *initial definition* of an intra-SM MD link on a GSM?

- If **yes**, SKIP to Step 6.
- If **no**, CONTINUE this procedure.

3. Determine if an intra-SM MD link is already provisioned by issuing the input message:

OP : STATUS , MD , SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM number.

- If the output indicates a **NONEXISTENT MD PATH**, CONTINUE this procedure.
- Otherwise, this procedure is inappropriate, as only one intra-SM MD link can be provisioned on a GSM. EXIT this procedure immediately.

4. Is the new termination of the intra-SM MD link to be made on an **existing** CCS channel group?

- If **yes**, CONTINUE this procedure.
- If **no**, SKIP to Step 6.

5. At an RC/V terminal, enter **16.11r** to access the CHANNEL GROUP ASSIGNMENT DEFINITION view in

REVIEW mode.

Specify the key fields from the proposed target PSU termination:

SM	(target GSM number)
SHELF	(PSU shelf number)
CHGRP	(target channel group)

Is the view displayed?

- If **no**, EXIT this procedure immediately and re-evaluate the choice of PSU termination.
- If **yes**, and the proposed channel group member is **not** assigned, SKIP to Step 7.
- If **yes**, but the proposed channel group member is **already** assigned, EXIT this procedure immediately and re-evaluate the choice of PSU termination.

Enter < to return to the forms menu and q to exit RC/V.

6. Use the procedure "Preparing the Packet Switch Unit for CCS Assignment," Procedure 13.1.8, to ensure that a PH3 is available for a **new** CCS channel group assignment required to assign the intra-SM MD link (the desired PSU shelf should be known before entering that procedure), and then CONTINUE this procedure.
7. At an RC/V terminal, enter **16.17i** to access the MESSAGE DELIVERY LINK view in INSERT mode.

Enter the following data for the new intra-SM MD link:

SM	(target GSM number)
SHELF	(PSU shelf associated with the intra-SM MD link)
CHANNEL GROUP	(channel group associated with the intra-SM MD link)
CH GP MEMBER	(channel group member associated with the intra-SM MD link)

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

8. Enter i to complete the insert.

When the insertion completes, "FORM INSERTED" flashes in the upper right corner of the screen and the cursor returns to the SM field.

A message

REPT CCS SM=xxx ODD BACKUP WARNING

(where **xxx** is the GSM number) warns you to backup the ODD promptly to avoid serious roll-forward problems, should the GSM undergo an initialization.

Enter < to return to the forms menu and q to exit RC/V.

9. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

10. Display the **1530,xxx MESSAGE DELIVERY LINK** page on an MCC/STLWS, where **xxx** is the target GSM number. The intra-SM MD link status displayed should be **DACT** (deactivated).

Enter the **3000** menu command to activate the MD link.

- If successful, the intra-SM MD link status will transition to active (ACT).
- If the activation fails, the failure should be investigated by using the procedures "Problem Analysis Strategies," Procedure 14.1 .

11. STOP. YOU HAVE COMPLETED THIS PROCEDURE.

Procedure 13.1.5: Define New Link Sets

OVERVIEW

Before any signaling routes (destination point codes) can be defined, at least one link set (LS) must be provisioned. Also, new LSs can be defined in established GSMs, as the need arises. This procedure can be used in either situation.

The value of the adjacent point code (APC), which is the far-end exchange terminating the new LS, must be negotiated according to local practices before entering this procedure.

PROCEDURE

1. Determine if the target SM/SM-2000 is already defined as a GSM by issuing the input message:

OP : CCS , GSM , SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM number.

- If the request fails (response "NG - GSM MISMATCH" or "NG - NO GLOBAL SM IN OFFICE"), the target SM/SM-2000 has not yet been defined as a GSM; EXIT this procedure immediately.

Use the procedure "Convert to a CCS Global Switching Module," Procedure 13.1.1 , to provision the GSM, and then RESTART this procedure.

- If the request succeeds, the GSM has already been defined and this procedure is appropriate; CONTINUE this procedure.

2. Display the **1532,xxx CCS LINK SET SUMMARY** page on an MCC/STLWS, where **xxx** is the target GSM number. All currently provisioned LSs on the GSM are displayed (the page is displayed, even if no LS is currently provisioned).

If the LS being added is **already** provisioned, review local administrative procedures to choose a new LS number, before continuing to the next step, or EXIT this procedure.

3. At an RC/V terminal, enter **16.5i** to access the SIGNALING LINK SET view in INSERT mode.

Enter the following data for the new LS:

LINK SET	(the new LS number)
GSM	(target GSM number)
APC	(the negotiated 9-digit APC value)

In 5E14 and later software releases, an additional optional field is present:

LINK TYPE	(link type label)

which may be populated with:

A for an access link to an adjacent STP,
E for an extended link to a secondary STP, or
F for a fully associated direct link to a SEP.

The read-only fields, PHYSICAL LINKS (the number of provisioned CCSLKs in the LS) and CLS COUNT

(number of CLSSs containing the LS), should both be *blank* at this point, as this is a new LS.

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

4. Enter **i** to complete the insert.

When the insertion completes, "FORM INSERTED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

5. Display the **1532,xxx CCS LINK SET SUMMARY** page on the MCC/STLWS, where **xxx** is the target GSM number. The newly provisioned LS is displayed in a *GROW* state.
6. Determine if the associated adjacent point code (APC) is already provisioned for the GSM by issuing the input message:

OP: CCS , DPC , DPCID=aaa , SM=xxx

on an MCC/STLWS, where **aaa** is the 9-digit APC number and **xxx** is the target GSM number.

- If the string *INVALID DPC* appears in the output, the APC is not yet defined as a DPC. Execute the procedure "Define New Destination Point Codes," Procedure 13.1.7 , to define the APC, using the newly inserted LS as the *NORMAL LINK SET*.
- Otherwise, the APC is already known to the GSM. Execute the procedure "Modify Link Sets Serving a DPC," Procedure 13.1.13 , to add the newly inserted LS as a valid route to that APC (as the *NORMAL LINK SET* or an *ALTERNATIVE LINK SET*, as appropriate).

Performing either of the previous procedures backs up the office dependent data (ODD), including the new LS definition.

7. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.6: Define a New Combined Link Set

OVERVIEW

This procedure defines a combined link set (CLS). Up to 8 CLSs can be defined for a GSM. Each CLS can have two LSs, but the LSs must already be provisioned on the GSM and must not be members of any other CLS. Use local procedures to determine the member LSs before starting this procedure.

PROCEDURE

1. Issue the input message:

OP:OFR,FORM=6005, DEVICE=xxx

on an MCC/STLWS to produce office records for the COMBINED SIGNALING LINK SET view. The destination **xxx** is described in "Signaling Link Provisioning Overview," Procedure 13.1.

Survey the output to determine all **CLSs** and the **LSs** that are already provisioned on the target GSM.

- If **eight CLSs are already provisioned on the GSM**, no more CLSs can be defined. This procedure is not appropriate; EXIT this procedure immediately.
- If the **target CLS is already provisioned on the GSM**, this procedure is not appropriate; EXIT this procedure immediately. The constituent LSs of this existing CLS can be modified (if desired) by the procedures "Redefine Combined Link Set Members," Procedure 13.1.12.
- If **either of the target member LSs is already assigned to another CLS**, this procedure is not appropriate as a given LS can only be a member of *one* CLS; EXIT this procedure immediately.
- Otherwise, CONTINUE this procedure.

2. Display the **1532,xxx CCS LINK SET SUMMARY** page on an MCC/STLWS, where **xxx** is the target GSM number, and observe the provisioned LSs displayed (the status of the LSs is irrelevant). Search for the **two** target LSs chosen for CLS provisioning.

- If one/both of the LSs required are **not** displayed, EXIT this procedure immediately.

Execute the procedures "Define New Link Sets," Procedure 13.1.5, to add the missing LSs (or choose a new constituent LS), and then REENTER this procedure.

- If **both** LSs are displayed, CONTINUE this procedure.

3. At an RC/V terminal, enter **16.7i** to access the COMBINED SIGNALING LINK SET view in INSERT mode.

Enter the following data for the new CLS:

CLS	(the new CLS number)
GSM	(target GSM number)
LS1	(first LS in the CLS)
LS2	(second LS in the CLS)

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

4. Enter **i** to complete the insertion.

When the insertion completes, "FORM INSERTED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

5. Issue the input message:

OP : CCS , CLS , SET=aaa , SM=xxx

on an MCC/STLWS, where **aaa** is the target CLS number and **xxx** is the GSM number. The output will specify that the new CLS is provisioned, with the member LSs as defined.

6. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

7. As an optional step, the new CLS can be added as a route to existing DPCs (or can replace one or both of the constituent LSs), by executing the procedures "Modify Link Sets Serving a DPC," Procedure 13.1.13 .
8. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.7: Define New Destination Point Codes

OVERVIEW

This procedure can be used to define a new DPC associated with a particular GSM. New signaling routes to a specific destination point code (DPC) can be defined at any time.

Before using this procedure, use local practices to determine the following:

- The normal LS/CLS (primary signaling route to access the DPC)
- Up to four alternative LS/CLSs (for use only if the primary LS/CLS is unusable)
- The DPC number (9-digit format).

The CLS/LSs designated as routes must already be provisioned.

PROCEDURE

1. Verify that the DPC being added has not already been defined for the target GSM.

Issue the input message:

OP: CCS, DPC, DPCID=aaa, SM=xxx

on an MCC/STLWS, where **aaa** is the 9-digit number of the DPC to be provisioned and **xxx** is the target GSM number.

- For pre-5E14 software releases, if the string **INVALID DPC** appears in the output, the target DPC is **not** yet defined; CONTINUE this procedure.
- For 5E14 and later software releases, if the string **NO DPC ROUTE SET PROVISIONED** appears in the output, the target DPC is **not** yet defined; CONTINUE this procedure.
- Otherwise the DPC is **already** provisioned; EXIT this procedure immediately.

2. Is a CLS to be used as a normal/alternate link set?

- If **yes**, CONTINUE this procedure.
- If **no**, SKIP to Step 4.

3. Determine if each CLS being used as a DPC route is defined on the GSM by issuing the input message:

OP: CCS, CLS, SET=aaa, SM=xxx

on an MCC/STLWS, where **aaa** is the CLS number and **xxx** is the target GSM number.

- If the string **NO DATA FOUND** appears in the response, the specified CLS does **not** exist; EXIT this procedure immediately.

The procedure "Define a New Combined Link Set," Procedure 13.1.6, can be used to provision the

desired CLS (or new LS/CLSs may be chosen as routes), and then this procedure can be reentered.

— Otherwise, record the constituent LSs for each target CLS, and CONTINUE this procedure.

4. If any ordinary LSs are to be used as routes to a DPC, display the **1532,xxx CCS LINK SET SUMMARY** page on an MCC/STLWS, where **xxx** is the target GSM number. Search for all of the LSs chosen for DPC routes (the status of these LSs is irrelevant).

— If **no** ordinary LSs are to be used as routes, SKIP to Step 6.

— If **all** target LSs are displayed (status is irrelevant), CONTINUE this procedure.

— If any of the LSs required are **not** displayed, EXIT this procedure immediately.

The procedure "Define New Link Sets," Procedure 13.1.5, can be used to provision the desired LS (or new LSs may be chosen for access), and then this procedure can be reentered.

5. Are both CLS(s) and ordinary LS(s) to be used as normal/alternate link sets?

— If **yes**, create a list of constituent LSs associated with CLSs (determined in Step 3), plus the ordinary LSs identified in Step 4.

If the list contains any duplication, EXIT this procedure immediately, because individual link sets assigned as routes to a DPC must be unique. Choose new CLS/LS candidates, then restart this procedure.

If the list contains no duplication, CONTINUE this procedure.

— If **no**, CONTINUE this procedure.

6. At an RC/V terminal, enter **16.10i** to access the SIGNALING POINT CODE view in INSERT mode.

Enter the following data for the new DPC:

POINT CODE	(new DPC in 9 digit format)
GSM	(target GSM number)
NORMAL LINK SET	(primary route LS/CLS)
ALTERNATE LINK SETS 1/2/3/4	(alternate route LS/CLS, as appropriate)

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

7. Enter **i** to complete the insert.

When the insertion completes, "FORM INSERTED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

8. Ensure that the DPC is recognized.

Issue the input message:

OP:CCS,DPC,DPCID=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the newly provisioned DPC and **xxx** is the target GSM number.

In pre-5E14 software releases, the output will specify that the DPC is ACCESSIBLE or INACCESSIBLE, dependent on the status of CLS/LS routes.

In 5E14 and later software releases, the output will specify that the DPC is ACCESS or INACCESS.

9. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

10. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.8: Preparing the Packet Switch Unit for CCS Assignment

OVERVIEW

In some cases, new PSU resources may have to be made available before intra-SM message delivery (MD) links or CCS signaling links (CCSLKs) can be assigned.

This procedure can be used to prepare for an individual CCSLK or intra-SM MD link assignment, or to prepare for the assignment of a large number of CCSLKs in a growth session. Groupings should be limited to the entire PSU on a specific SM-2000, or a PSU shelf on an SM (not SM-2000); for larger growth scenarios, multiple executions of this procedure are required, each adhering to the cited constraints.

Before using this procedure, investigate office records and consult engineering guidelines according to local practices. This procedure assumes the PSU channel group and member of each assignment is known and that a decision has been made to use existing PH3 or PH22 hardware or to grow new hardware. Prior to 5E14, only PH3 hardware can be provisioned for CCS use, but in 5E14 and later software releases, PH22 hardware becomes a viable alternative (and, if certain features are to be provisioned, only PH22 can be used). This procedure assumes that the type of PH hardware required is known in advance.

The following provisioning scenarios are allowed:

- The addition of a new member on an **existing** CCS channel group.
- The use of **spare** PH3s or PH22s already equipped on the GSM that are designated as **minimum shelf spares** for reliability.

This is a valid choice only if the office sparing philosophy has changed, or the new assignment is an *emergency action* to alleviate severe CCS congestion problems. Long term action should include the growth of new PH22 hardware to achieve the minimum sparing philosophy appropriate for PSU operation.

- The growth of **new PH3 or PH22 hardware** and possible **new PSU shelves** on the GSM.
- In **non-SM-2000** GSMs, the reservation of peripheral interface data bus (PIDB) timeslots.

PROCEDURE

1. Where are the new intra-SM MD link or CCSLK assignments to be made?
 - If assignments are to be made on an **existing** CCS channel group (the calling procedure has verified that the target channel group member is actually available for assignment), SKIP to step 8.
 - If assignments are to be made on a **new** channel group, CONTINUE the procedure.
2. Will the new channel group use existing spare PH3 or PH22 hardware, or require new hardware to be grown?
 - If **new PH3 or PH22 hardware** needs to be grown, SKIP to Step 6.
 - If **existing spare PH3 or PH22 hardware** is to be used, CONTINUE this procedure.
3. At an RC/V terminal, enter **22.16r** to access the PSU PROTOCOL HANDLER CHANNEL GROUP ASSIGNMENT view in REVIEW mode.

Specify the key fields from the proposed target PSU termination:

SM	(target GSM number)
PSU	(0 must be entered for the PSU number)
SHELF	(target PSU shelf number)

All the other fields are populated with current values.

Observe the value of the read-only field PH3 AVAIL or PH22 AVAIL, as appropriate (which is the number of PH3s or PH22s on the shelf available for channel group assignment, *excluding* designated spares).

- If the number of available PH3s or PH22s on the designated PSU shelf is **greater** than the number required by this provisioning session, SKIP to Step 7.
- Otherwise, if the intended **assignment is on shelves 1 to 4**, SKIP to Step 5.
- Otherwise, if the intended **assignment is on shelf 0**, CONTINUE this procedure.

Enter < to return to the forms menu.

CAUTION: Performing Steps 4 or 5 will alter the current minimum spare philosophy for the affected PSU shelf. This could have adverse effects on PSU reliability and should be executed on an emergency basis only as a temporary measure.

4. At an RC/V terminal, enter **22.2u** to access the PACKET SWITCH UNIT view in UPDATE mode.

Specify the key fields:

SM	(target GSM number)
PSU	(0 must be entered for the PSU number)

All the other fields are populated with current values and the string *Enter Update, Change, Validate, screen#, or Print:* is produced.

Check the value of the PH3 MIN SPARE or PH22 MIN SPARE field, as appropriate.

- If the number of minimum PH3 or PH22 spares is **0**, there is no PH3 or PH22 available for CCS assignment; EXIT this procedure and re-evaluate sparing strategies.
- If the number of PH3 or PH22 spares is **1**, the last spare PH3 or PH22 could be made available for CCS assignment, but this would reduce the number of spare PH3s or PH22s on the shelf to zero and would cause severe reliability problems.
- Otherwise, multiple spare PH3s or PH22s exist and could be made available for temporary CCS assignment.

Enter **c** to start change mode. The expected response is *Change field:* string. Enter the number of the PH MIN SPARE field to move the cursor to that field.

Enter a new value, which is the **current** value **decremented by one** for **each spare** PH3 or PH22 to be used for CCS functionality (minimum value 0). The expected response is *Change field:* string.

Enter < to return to the update command line and **u** to complete the update. When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu and **q** to exit RC/V. SKIP to step 7.

5. At an RC/V terminal, enter **22.3u** to access the PACKET SWITCH UNIT SHELF 1-4 view in UPDATE mode.

Specify the key fields from the proposed target PSU termination:

SM	(target GSM number)
PSU	(0 must be entered for the PSU number)
SHELF	(target PSU shelf number)

All the other fields are populated with current values and the string *Enter Update, Change, Validate, screen#, or Print:* is produced.

Check the value of the PH3 MIN SPARE or PH22 MIN SPARE field, as appropriate.

- If the number of minimum PH3 or PH22 spares is **0**, there is no PH3 or PH22 available for CCS assignment; EXIT this procedure and re-evaluate sparing strategies.
- If the number of PH3 or PH22 spares is **1**, the last spare PH3 or PH22 could be made available for CCS assignment, but this would reduce the number of spare PH3s or PH22s on the shelf to zero and would cause severe reliability problems.
- Otherwise, multiple spare PH3s or PH22s exist and could be made available for temporary CCS assignment.

Enter **c** to start change mode. The expected response is *Change field:* string. Enter the number of the PH MIN SPARE field to be updated to move the cursor to that field.

Enter a new value, which is the **current** value **decremented by one** for **each spare** PH3 or PH22 to be used for CCS functionality (minimum value 0). The expected response is *Change field:* string.

Enter **<** to return to the update command line and **u** to complete the update. When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V, and SKIP to step 7.

6. If new PH3 or PH22 hardware will be used for CCS services to be provisioned, execute *PROCEDURE 3.95, Perform Protocol Handler (PH) Growth* procedure in 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures - Growth* to grow in the required number of PH3s or PH22s on the target GSM before continuing with these procedures.

PROCEDURE 3.95 will accommodate the growth of new PH3 or PH22 hardware (for CCS channel group assignment, as well as new spares), new shelf hardware (if required) and the designation of minimum shelf spares for reliability. The procedure will fail if an attempt is made to install more than 15 PHs per shelf or more than 5 shelves on the PSU. If total hardware exhaust is encountered, the only way to free hardware resources for CCS usage is to degrow or reengineer existing services using PH3 or PH22 hardware.

Record the shelf location of new hardware to be used for intra-SM MD link or CCSLK assignments.

7. At an RC/V terminal, enter **22.16u** to access the PSU PROTOCOL HANDLER CHANNEL GROUP ASSIGNMENTS view in UPDATE mode.

Specify the key fields from the proposed target PSU termination:

SM	(target GSM number)
PSU	(0 must be entered for the PSU number)
SHELF	(target PSU shelf number)

All the other fields are populated with current values and the string *Enter Update, Change, Validate, or Print:* is produced.

Check the value of the read-only field PH3 AVAIL or PH22 AVAIL, as appropriate (which is the number of PH3s or PH22s on the shelf available for channel group assignment, *excluding* designated spares).

- If the available PH3s or PH22s on the designated PSU shelf is **0**, an error has been made in initial channel group assignment instructions, or in the preparation of PSU hardware. EXIT this procedure immediately and review PH channel group assignments. When new assignments are determined, REENTER this procedure.
- Otherwise, enter **c** to start change mode. The expected response is the *Change field:* string. Enter the **number of the field** to be updated, corresponding to the new **channel group** to be assigned to move the cursor to that field.

Enter a **PH3** or **PH22** in that field. The expected response is the *Change field:* string.

Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen. Note that the *GRP TYPE* for the target channel group is populated as *NULL* (until actual CCSLK or MD link assignments are made).

Enter **<** to return to the forms menu and **q** to exit RC/V.

8. Answer the following questions, making the appropriate choice.

- If this procedure is preparing for an **intra-SM MD link assignment**, SKIP to Step 13.
- If this procedure is preparing for a **CCSLK assignment on an SM-2000 type of GSM**, SKIP to Step 13.
- Otherwise, CONTINUE this procedure.

9. On an SM (not SM-2000), it is required that peripheral interface bus (PIDB) timeslots to the PSU from a specific data interface (DI) be reserved in advance, to be used by provisioned CCSLKs as a permanent nailed-up resource.

The technician has two choices, specifically:

- The steps that follow can be executed to proactively reserve the required PIDB timeslots. The steps require a substantial amount of analysis, but are strongly suggested, if a large number of new CCSLKs are to be defined.
- The alternative is to proceed with the provisioning of CCSLKs, using the procedure "Define New Link Set Members," Procedure 13.1.10, *assuming* spare reserved PIDB timeslots exist. If such timeslots are not reserved, recent change will fail; detailed instructions in the cited procedure will provide for the "ad hoc" reservation of timeslots. This method is the least time consuming, if only one/two CCSLKs are to be provisioned.

Based on the above information, proceed as follows:

- If **proactive** PIDB timeslot reservation is desired, CONTINUE this procedure.
- If **reactive** PIDB timeslot reservation (in response to a recent change failure) is desired, SKIP to Step 13.

10. The first step in engineering PIDB timeslots is to determine the number of PIDBs assigned to each shelf in the target PSU and determine the corresponding DI.

Proceed as follows:

- Display the **PACKET SWITCH UNIT** page on an MCC/STLWS, using the command **1186,xxx**, where **xxx** is the target GSM. Record the **numbers** of all **equipped** PSU shelves displayed.
- If **shelf 0** is equipped, enter **22.2r** at an RC/V terminal, to access the PACKET SWITCH UNIT view in REVIEW mode.

Specify the key fields:

SM	(target GSM number)
PSU	(0 must be entered for the PSU number)

After fields are populated, move to *screen 2* (DATA INTERFACE heading).

Determine the number of PIDBs assigned to shelf 0 (each **pair** of populated rows corresponds to **one** PIDB), and the terminating DI (the **DI** is the value 0 or 1 present in the **DI/TSIS** column for all entries). Then, enter < to return to the forms menu.

- For each equipped shelf in the range **1-4**, enter **22.3r** at an RC/V terminal, to access the PACKET SWITCH UNIT SHELF 1-4 view in REVIEW mode.

Specify the key fields:

SM	(target GSM number)
PSU	(0 must be entered for the PSU number)
SHELF	(target PSU shelf number)

After fields are populated, move to *screen 2* (DATA INTERFACE heading).

Determine the number of PIDBs assigned to each equipped shelf 0 (each **pair** of populated rows corresponds to **one** PIDB), and the terminating DI (the **DI** is the value 0 or 1 present in the **DI/TSIS** column for all entries). Then, enter < to return to the forms menu.

- Issue the input message:

OP : STATUS , PSUTSCOUNT , SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM. Determine the number of PIDB timeslots that must be reserved on a **per-shelf** basis to support all *current* nailed-up services on the PSU (this does **not** include any new CCSLKs being provisioned now).

- Finally, from all data gathered, fill in the following table:

AA = PSU shelf number where CCSLK growth is to occur

BB = DI associated with shelf **AA**

CC = number of PIDBs provisioned for shelf **AA**

DD = number of **new** CCSLKs to be provisioned on shelf **AA**

EE = number of **current** nailed-up PIDB timeslots on shelf **AA**

FF = number of **current** nailed-up PIDB timeslots on **all** shelves using DI **BB**

Based on the values calculated, perform the following actions:

- If $DD + EE > 32 \times CC$, there will be insufficient *physical* PIDB timeslots on the shelf to accomplish the desired growth. EXIT this procedure immediately, replan the assignment of some new CCLKs to other PSU shelves, or degrow some existing nailed-up services on the target PSU shelf, or grow in an additional PIDB to the target shelf (use *PROCEDURE 3.89 Packet Switch Unit Peripheral Interface Bus Growth Procedure* in the 235-105-231, 5ESS®-2000 Switch Hardware Change Procedures - Growth document). Then, reenter this procedure.
- Otherwise, CONTINUE this procedure.

11. Based on data derived in the previous step, enter **22.2r** on an RC/V terminal to access the PACKET SWITCH UNIT view in REVIEW mode.

Specify the key fields:

SM	(target GSM number)
PSU	(0 must be entered for the PSU number)

After all fields are populated, request a review of screen **3** (DI0 PSU TSIU TIMESLOTS screen), if **BB** is **DI 0**, or screen **4** (DI1 PSU TSIU TIMESLOTS screen), if **BB** is **DI 1**. Every **1** present in any **RPTSS** row represents PIDB timeslot on the target DI that is reserved for a nailed-up service (a **0** indicates the timeslot is not currently reserved), and the **AVAILABLE TS** row indicates the number of DI timeslots that are available for PSU PIDB use (the 32 columns represent individual PIDB timeslots).

Set the variable **GG** to be equal to the total number of current reserved timeslots on DI **BB** (this the total numbers of **1s** in **all** RPTSS rows).

Enter < to return to the forms menu.

Based on the values calculated, perform the following actions:

- If $DD + FF > GG$, more PIDB timeslots must be reserved, so CONTINUE this procedure.
- Otherwise, sufficient spare reserved timeslots are available, SKIP to Step 13.

12. At this point, it is known that $DD + FF - GG$ (cited variables derived in previous steps) additional PIDB timeslots must be reserved on the target DI.

Enter **22.2u** on an RC/V terminal to access the PACKET SWITCH UNIT view in UPDATE mode.

Specify the key fields:

SM	(target GSM number)
PSU	(0 must be entered for the PSU number)

After all fields are populated with current values, the string *Enter Update, Change, Validate, screen#, or Print:* will be produced.

Move to screen **3** (DI0 PSU TSIU TIMESLOTS screen) if **BB** is **DI 0**, or screen **4** (DI1 PSU TSIU TIMESLOTS screen) if **BB** is **DI 1**. The intent of this update is to replace $DD + FF - GG$ of the **0** entries in the timeslot map with **1s**. For any given **0** to be changed, the **AVAILABLE TS** count for that **column** must be greater than zero. It is really irrelevant as to which **RPTSS rows** are altered, but the **number of 1s** in a given **column** should be balanced as much as possible (i.e., every column should have **one 1** before any column has a **second 1** assigned, and every column should have **two 1s** before any column has a **third 1** assigned, and so forth).

Enter **c** (for change mode), and enter the number associated with the **DI0/1 PSU TSIU TIMESLOT** field; choose an appropriate **RPTSS** row, where **0s** can be changed to **1s**, according to the guidelines above. Repeat this procedure until all the required changes have been made.

Enter **<** to return to the update command line, and **u** to complete the update. When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen. Enter **<** to return the forms menu, and **q** to quit RC/V.

13. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS. When the backup completes, RETURN to the calling procedure.

14. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.9: Convert PH3 to PH22 Hardware

OVERVIEW

In 5E14 and later software releases, the PH version 22 (PH22) hardware type is available for CCS use. Conversion from PH3 to PH22 may be desired to increase performance, or be required to support 5E14 MTP features. This procedure coordinates such an effort, minimizes disruption of service, and applies to channel groups supporting an intra-SM MD link or CCSLKs.

WARNING: Some actions taken during the conversion process can cause partial/total loss of CCS services on the GSM (further warnings are provided in the appropriate procedural steps), so advance preparation and quickly executed RC transactions are necessary to minimize planned outage times.

PROCEDURE

1. Are there spare slots on existing PSU shelves, or will a new shelf be grown, to accommodate new PH22 hardware (including appropriate shelf spares of this PH hardware type)?
 - If **yes**, SKIP to Step 3.
 - If **no**, but all PH3s on the shelf will be replaced with PH22s, and there is at least one SPARE PH3 on the shelf, CONTINUE this procedure.
 - Otherwise, EXIT this procedure, as no additional protection of CCS service can be provided beyond simple intra-SM MD link degrowth (see "Delete Intra-SM Message Delivery Link," Procedure 13.1.19) or CCSLK degrowth (see "Delete Link Set Members," Procedure 13.1.15) on existing PH3 hardware, followed by degrowth of the PH3 hardware itself (Procedure 4.20, Protocol Handler (PH) Degrowth in 235-105-331, 5ESS®-2000 Switch Hardware Change Procedures - Degrowth). Then new PH22 hardware can be grown (Procedure 5.25, Protocol Handler (PH) Growth in 235-105-231, 5ESS®-2000 Switch Hardware Change Procedures - Growth), and regrow the intra-SM MD link or CCSLK, as appropriate, on a new PH22 channel group (see "Define Intra-SM Message Delivery Link," Procedure 13.1.4 , or "Define New Link Set Members," Procedure 13.1.10 , respectively).

If this case is encountered, the PH sparing philosophy suggested in engineering guidelines has *not* been implemented. It is suggested that the overall sparing philosophy for the PSU be reviewed before taking any further action.

2. Display the **118y,xxx PSU 0 SHELF y** page on an MCC/STLWS, where **y** is the PSU shelf in the range 0-4 on the target GSM **xxx**, that contains the SPARE PH3 of interest.

Observe the status of the spare PH3 on the shelf (either OOS or STBY), and manually remove it by issuing the input message:

RMV:PSUPH=xxx-0-y-a

where **a** is the target physical PH number.

Next degrow the target PH3, using Procedure 4.20, Protocol Handler (PH) Degrowth in 235-105-331, 5ESS®-2000 Switch Hardware Change Procedures - Degrowth, and then CONTINUE this procedure.

WARNING: Until the conversion procedure is complete, this step may have deleted the only spare PH3 on the target PSU shelf, reducing reliability, should a fault occur.

3. Use the procedure "Preparing the Packet Switch Unit for CCS Assignment," Procedure 13.1.8 , to prepare the PSU environment for conversion to PH22 hardware.

This includes the growth of new PH22 hardware, as if the intra-SM MD link or CCSLKs to be moved are treated as new growth. The exception is if PH3 channel groups to be converted to PH22s reside on the same shelf (not an SM-2000), where new PIDB timeslot reservations will not be required.

4. Select a PH3 CCS channel group to be converted to a PH22 hardware type (bias the order of conversion as listed).

— If an MD or MDST7 channel group is to be converted, CONTINUE this procedure.

— If an ST7 channel group is to be converted, SKIP to Step 6.

5. There is no way to move the intra-SM MD link to a new channel group without affecting service.

First, delete the existing intra-SM MD link on an MD/MDST7 PH3 channel group, using the procedure "Delete Intra-SM Message Delivery Link," Procedure 13.1.19 .

Next, reprovision the intra-SM MD link on the new PH22 channel group, using the procedure "Define Intra-SM Message delivery Link," Procedure 13.1.4 .

CAUTION: All ISUP calls/TCAP activities using the affected PSU platform on the target GSM will cease until the intra-SM MD link conversion is complete, so speed is critical.

If the channel group converted was an MD type, SKIP to Step 10; otherwise, CONTINUE this procedure.

6. At an RC/V terminal, enter **16.11r** to access the CHANNEL GROUP ASSIGNMENT DEFINITION view in REVIEW mode.

Specify the key fields from the PH3 channel group to be converted:

SM	(target GSM number)
SHELF	(PSU shelf number)
CHGRP	(target PH3 channel group)

Record the resident link set/members, and then enter < to return to the forms menu and q to exit RC/V.

7. For each of the link sets identified in the previous step, display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on an MCC/STLWS, where **aaa** is the target link set number on GSM **xxx**.

For a target link set, if *at least* half the provisioned members are *not* ACT and one or more members are OOS (while counting, assume the CCSLK to be converted is OOS, regardless of actual status), recover sufficient CCSLKs in the target link set to satisfy these criteria, using "Clear GSM Signaling Link Problems," Procedure 14.2.1 .

Repeat this scenario for all identified link sets with CCSLKs on the channel group to be converted, and then CONTINUE this procedure.

8. For each CCSLK identified in Step 6, use procedure "Modify Link Member Characteristics," Procedure 13.1.14 to change the existing PH3 termination to the new PH22 channel group.

9. If desired, degrow the PH3 no longer being used for CCS services (this may be necessary to free PSU shelf slots for further PH22 growth). Use *Procedure 4.20, Protocol Handler (PH) Degrowth* in 235-105-331, *5ESS®-2000 Switch Hardware Change Procedures - Degrowth*.

10. Are there further PH3 channel groups to be converted to a PH22 hardware base?
 - If **yes**, RETURN to Step 1.
 - If **no**, CONTINUE this procedure.
11. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.10: Define New Link Set Members

OVERVIEW

This procedure can be used to define new signaling links (CCSLKs) on a specific GSM. New CCSLKs can be added to an existing link set (LS), and activated for use, at any time.

Before entering this procedure, check the following data, per local office practices:

- The CCSLK identified must not already be provisioned (identified by LS and member number in the range 0-7).

NOTE: For 5E14 and later software releases, the member number has a range of 0-15.

- A PH termination on the GSM, designated by PSU shelf/channel group/member number in the range 0-3, must be an unassigned member of an existing CCS channel group, or a member of a CCS channel group not yet defined.
- A signaling data link (SDL) access termination on a DFI/DNU-S facility, which must reside on the target GSM:

— For DFI/DFI2 access, the SDL is identified by a digital equipment number (DEN) with the following components:

DEN=a-b-c-d where **a** is the target GSM number, **b** is the DLTU (digital line trunk unit) number, **c** is the DFI (digital facility interface) number, and **d** is the DS0 channel number, in the range 1-48.

The designated DEN must be an **unassigned** port on an **equipped** DFI facility.

— For DNU-S access, the SDL is identified by a network equipment number (NEN) with the following components in pre-5E13 software releases:

NEN=a-b-x-y-vv-c

where **a** is the target GSM number, **b** is the digital network unit - SONET (DNU-S) number, **x** is the data group (DG), **y** is the synchronous transport signal (STS) number, **vv** is the virtual tributary 1.5 (VT1.5), and **c** is the DS0 channel number in the range 1-24.

For 5E13 and later software releases, the NEN definition is altered to redefine synchronous transport signal and virtual tributary numbering conventions to accommodate Bellcore standards, specifically:

NEN=a-b-x-s-y-g-m-c

where **s** is the SONET termination equipment (STE) number, **g** is the virtual tributary group (VTG) number, and **m** is the virtual tributary member (VTM) number.

The NEN must be an **unassigned** port on an **equipped** VT1.5 facility.

- The transmission rate of the DS0 channel (56 Kbps or 64 Kbps) must be known.
- The signaling link code (SLC) associated with the CCSLK must be negotiated with the APC.
- The maximum message signaling unit (MSU) transport rate must be known.
- If default congestion thresholds are not acceptable, new values must be chosen according to local practices. For guidance see 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)*.

It is assumed that compatible link growth activities have occurred in the far-end APC exchange (or activation will not be possible).

PROCEDURE

1. Verify the target CCSLK does not already exist, and that the parent LS is provisioned, by displaying the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on an MCC/STLWS, where **aaa** is the parent LS number and **xxx** is the target GSM number.

Respond as follows:

- If the page is **not** displayed or the string **WRONG LINKSET** appears on the page, EXIT this procedure immediately and provision a new LS using the procedure "Define New Link Sets," Procedure 13.1.5, or choose a new parent LS, and then REENTER this procedure.
- If the page is displayed, and the target CCSLK **already exists**, EXIT this procedure immediately and choose a new CCSLK to be provisioned.
- Otherwise, CONTINUE this procedure.

2. Is the CCSLK to be provisioned on a new CCS channel group?

- If **yes**, SKIP to Step 4.
- If **no**, CONTINUE this procedure.

3. At an RC/V terminal, enter **16.11r** to access the CHANNEL GROUP ASSIGNMENT DEFINITION view in REVIEW mode.

Specify the key fields from the proposed target PSU termination:

SM	(target GSM number)
SHELF	(PSU shelf number)
CHGRP	(target channel group)

Is the view displayed?

- If **no**, EXIT this procedure immediately and re-evaluate the choice of PSU termination.
- If **yes**, and the proposed channel group member **is already assigned**, EXIT this procedure and re-evaluate the choice of PSU termination.
- If **yes**, and the proposed channel group member **is not assigned** and termination is on an **SM** (not an SM-2000), CONTINUE this procedure.
- If **yes**, and the proposed channel group member **is not assigned** and termination is on an **SM-2000**, SKIP to Step 5.

Enter < to return to the forms menu and q to exit RC/V.

4. Use the procedure "Preparing the Packet Switch Unit for CCS Assignment," Procedure 13.1.8, to prepare the PSU environment for CCSLK provisioning (possibly to prepare for a new channel group, or to reserve

PIDB timeslots). Then, REENTER this procedure at Step 5.

5. What access hardware is used to terminate the SDL?

- If access is through a **DNU-S**, SKIP to Step 7.
- If access is through a **DFI2**, CONTINUE this procedure.

6. At an RC/V terminal, enter **7.41** to access the T1 CHANNEL USAGE view in REVIEW mode.

Specify the key fields from the proposed target SDL DEN termination:

SM	(target GSM number)
DLTU	(digital line trunk unit number)
DFI	(digital facility interface number)
FAC IND	(should be 0 for DFI terminations, or 1 for DS0 channels in the range 1-24 on a DFI2, or 2 for channels in the range 25-48 on a DFI2)

Is the view displayed?

- If **no**, refer to the *PROCEDURE 3.25, Perform DFI/DFI-2 Growth* procedure in 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures - Growth* to grow in a new DFI2, or choose a new SDL termination.
- If **yes**, and the proposed DS0 channel is **already assigned**, EXIT this procedure and choose another SDL termination.
- If **yes**, and the proposed DS0 channel is **not** assigned, SKIP to Step 8.

7. At an RC/V terminal, enter **7.42** to access the DS1 CHANNEL USAGE view in REVIEW mode.

Specify the key fields from the proposed target SDL NEN termination, which has the following format in pre-5E13 software releases:

SM	(target GSM number)
DNU-S	(digital network unit number)
DATA GROUP	(data group number)
STS	(synchronous transport signal number)
VT	(VT1.5 facility)

For 5E13 and later software releases, the key fields change to reflect new synchronous transport signal and virtual tributary numbering conventions, specifically:

SM	(target GSM number)
DNU-S	(digital network unit number)
DATA GROUP	(data group number)
STE	(SONET termination equipment number)
STS	(synchronous transport signal number)
VT GROUP	(virtual tributary group)
VT MEMBER	(virtual tributary member)

Is the view displayed?

- If **no**, refer to the *PROCEDURE 3.196, Perform DNU-S Service TMUX Pack Growth* procedure in 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures - Growth* to grow in a new DNU-S facility, or choose a new SDL termination.
- If **yes**, and the proposed DS0 channel is **already assigned**, EXIT this procedure and choose another

SDL termination.

— If **yes**, and the proposed DS0 channel is **not** assigned, CONTINUE this procedure.

8. At an RC/V terminal, enter **16.6i** to access the SIGNALING LINK SET MEMBER view in INSERT mode.

Enter the following data for the new CCSLK:

LINK SET	(parent LS number of the new CCSLK)
MEMBER	(member number of the new CCSLK)
GSM	(target GSM number)
SLC	(negotiated signaling link code)
RATE	(56 Kbps or 64 Kbps transmission rate)
OE TYPE	(D for DFI access, or N for DNU-S access)
OE	(DEN for DFI access, or NEN for DNU-S access)
TRANSM RATE	(maximum number of MSUs to be transmitted in a 20 ms window, noting zero means unlimited)
SHELF	(PSU shelf to terminate the CCSLK)
CHANNEL GROUP	(PSU channel group to terminate the CCSLK)
CH GP MEMBER	(PSU channel group member to terminate the CCSLK)
H RET ONSET	(congestion thresholds - see TG5)
H RET ABATE	(congestion thresholds - see TG5)
H RET DISC	(congestion thresholds - see TG5)
H TRAN ONSET	(congestion thresholds - see TG5)
H TRAN ABATE	(congestion thresholds - see TG5)
H TRAN DISC	(congestion thresholds - see TG5)
M RET ONSET	(congestion thresholds - see TG5)
M RET ABATE	(congestion thresholds - see TG5)
M RET DISC	(congestion thresholds - see TG5)
M TRAN ONSET	(congestion thresholds - see TG5)
M TRAN ABATE	(congestion thresholds - see TG5)
M TRAN DISC	(congestion thresholds - see TG5)
L RET ONSET	(congestion thresholds - see TG5)
L RET ABATE	(congestion thresholds - see TG5)
L RET DISC	(congestion thresholds - see TG5)
L TRAN ONSET	(congestion thresholds - see TG5)
L TRAN ABATE	(congestion thresholds - see TG5)
L TRAN DISC	(congestion thresholds - see TG5)

See 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)* for details.

Enter predetermined values, or **RETURN** to accept default values. When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

9. Enter **i** to complete the insert, and react to the following events:

— If the insertion completes successfully, "FORM INSERTED" flashes on the upper right corner of the screen.

In this case, enter **<** to return to the forms menu and **q** to quit RC/V. Wait for a message

REPT CCS SM=xxx ODD BACKUP WARNING

(where **xxx** is the target GSM) to appear on the ROP, warning you to backup the ODD promptly to avoid serious roll-forward problems, should the GSM undergo an initialization; SKIP to Step 11.

— Otherwise an insert failure has occurred. CONTINUE this procedure.

10. If the insert fails, look for the following error messages, and respond as instructed:

— If the error message

The sum of Nailups (##), RPA (##), and ODB (##) timeslots cannot exceed ##;

appears, where **##** are numerical values appropriate for the current PSU shelf configuration, there are insufficient *physical* PIDB timeslots on the shelf to accomplish the desired growth.

Enter < to return to the forms menu, **q** to quit RC/V, and EXIT this procedure immediately. Replan the assignment of some new CCSLKs to other PSU shelves, or degrow some existing nailed-up services on the target PSU shelf, or grow in an additional PIDB to the target shelf (use *PROCEDURE 3.89 Packet Switch Unit Peripheral Interface Bus Growth Procedure* in the 235-105-231, 5ESS®-2000 Switch Hardware Change Procedures - Growth document). Then, reenter this procedure.

— If the error message

All PSU TSIU TIMESLOTS (vw 22.2) are used

appears, no further PSU timeslots can be reserved for nailed-up services on the target GSM; this message *cannot* appear on an SM-2000.

Enter < to return to the forms menu, **q** to quit RC/V, and EXIT this procedure immediately. The only way to provision new CCSLKs is to degrow some existing nailed-up services on the target PSU. Perform the required degrowth, and then reenter this procedure.

— If the pair of error messages

**Not enough unique PSU TSIU TIMESLOTS (vw 22.2)
reserved on DI AA for SM xxx**

**Reserving PSU TSIU TIMESLOT BB in RPTSS CC will
provide an additional timeslot**

appears, where **xxx** is the target GSM, an insufficient number of reserved PIDB timeslots to the target PSU shelf exist to accommodate the new CCSLK growth; this message pair *cannot* appear on an SM-2000.

Enter < to return to the forms menu, and enter **22.2u** to access the PACKET SWITCH UNIT view in UPDATE mode.

Specify the key fields:

SM	(target GSM number)
PSU	(0 must be entered for the PSU number)

After all fields are populated with current values, the string *Enter Update, Change, Validate, screen#, or Print:* will be produced.

Move to screen **3** (DI0 PSU TSIU TIMESLOTS screen), if **AA** in the error message is **0**, or screen **4** (DI1 PSU TSIU TIMESLOTS screen), if **AA** is **1**. Enter **c** (for change mode), and enter the number associated with the **DI0/1 PSU TSIU TIMESLOT** field; choose a row corresponding to **RPTSS BB** specified in the error message. Change the **0** in column **CC** specified in the error message to a **1**.

Enter < to return to the update command line, and **u** to complete the update. When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen. Enter < to return the forms menu, and RETURN to Step 8 to reattempt the CCSLK provisioning.

— Otherwise, contact the next level of technical support, according to local practices.

11. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

12. Display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on the MCC/STLWS, where **aaa** is the LS number (parent of the newly provisioned CCSLK), and **xxx** is the target GSM number.

The newly provisioned CCSLK will be present, in a deactivated (DACT) state.

Attempt to activate the CCSLK, by entering **3xx**, where **xx** is the CCSLK member number.

If the CCSLK does not successfully restore, the far-end exchange may not have completed its growth procedure for the link. To investigate the failure, use the procedures in "Problem Analysis Strategies," Procedure 14.1 .

13. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.11: Redefine Intra-SM Message Delivery Link Termination

OVERVIEW

There is no direct update available to change the PSU channel group termination of the intra-SM MD link on a specific GSM, but this procedure performs the task.

CAUTION: All ISUP calls/TCAP activities using the PSU platform on the target GSM will cease for the duration of the conversion procedure.

PROCEDURE

1. Delete the existing intra-SM MD link on the target GSM, using the procedure "Delete Intra-SM Message Delivery Link," Procedure 13.1.19 .
2. Reprovision the intra-SM MD link on the new PSU channel group termination on the target GSM, using the procedure "Define Intra-SM Message Delivery Link," Procedure 13.1.4 .
3. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.12: Redefine Combined Link Set Members

OVERVIEW

This procedure redefines the member link sets (LSs) in a combined link set (CLS). The new LSs should be determined before entering this procedure and those replacement LSs must already be provisioned and not be a member of another CLS.

CAUTION: UNCONDITIONAL removals of all members of existing and replacement LSs associated with the target CLS may impact CCS operation.

PROCEDURE

1. To update component LSs, the CLS must already be defined on the target GSM. Issue the input message:

OP: CCS , CLS , SET=aaa , SM=xxx

on an MCC/STLWS, where **aaa** is the target CLS number and **xxx** is the GSM number.

- If the string **NO DATA FOUND** appears in the response, this procedure is not appropriate because the target CLS is not currently defined; EXIT this procedure immediately.

Use the procedure "Define a New Combined Link Set," Procedure 13.1.6 , to define a new CLS, or choose a different CLS to be modified.

- Otherwise, the target CLS already exists and the member LSs may be modified. Record existing LSs and CONTINUE this procedure.

2. Display the **1532,xxx CCS LINK SET SUMMARY** page on an MCC/STLWS, where **xxx** is the target GSM number, and observe the LSs displayed. Verify that **both** of the LSs chosen for the new CLS composition are displayed.

- If one or both of the LSs required are **not** displayed, EXIT this procedure immediately.

Use the procedure "Define New Link Sets," Procedure 13.1.5 , to add the missing LSs (or choose new ones).

- If **both** LSs appear, CONTINUE this procedure.

3. Issue the input message for **one or both** of the replacement LSs.

OP: CCS , LSCLS , LS=aaa , SM=xxx

on an MCC/STLWS, where **aaa** is the replacement LS number and **xxx** is the target GSM number.

- If the target LS is identified as a member of **another CLS**, this procedure is not appropriate because a LS can be a member of only one CLS. EXIT this procedure immediately, and choose a new replacement LS.

- Otherwise, CONTINUE this procedure.

4. All members of the existing and replacement LSs must be deactivated before making any RC/V changes. On the *1532 CCS LINK SET SUMMARY* MCC page, sequence through **existing** and **replacement** LSs associated with the target CLS.

If an identified LS is *not GROW*, execute the **2xxx** menu command, where **xxx** is the LS number to *UNCONDITIONALLY* deactivate all CCSLKs in the LS; authorize the deactivation when warned of the danger by MCC prompts.

5. At an RC/V terminal, enter **16.7u** to access the COMBINED SIGNALING LINK SET view in UPDATE mode.

Specify the key fields:

CLS	(target combined link set number)
GSM	(target GSM number)

All the other fields are populated with current values, and the string *Enter Update, Change, Validate, or Print:* is produced.

6. Enter **c** to start change mode. The expected response is *Change field:* string. Enter the number of the LS1 (or LS2) field to move the cursor to that field.

Enter the new LS value. The expected response is *Change field:* string.

7. Have all the required component LSs been updated?

— If **no**, RETURN to Step 6 to update the other LS.

— If **yes**, CONTINUE this procedure.

8. Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

9. Issue the input message:

OP: CCS, CLS, SET=aaa, SM=xxx

on an MCC/STLWS, where **aaa** is the target CLS number and **xxx** is the GSM number.

The output specifies the target CLS is provisioned, with the *new* member LSs defined.

10. Back up the new ODD by entering the input message:

BKUP: ODD

on an MCC/STLWS.

11. The LSs must be activated by returning to the *1532 CCS LINK SET SUMMARY* MCC page and sequencing through **original** and **new** LSs associated with the target CLS.

If the LS is *not GROW*, execute the **3xxx** menu command, where **xxx** is the identified LS number, to activate all CCSLKs in the LS.

12. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.13: Modify Link Sets Serving a DPC

OVERVIEW

Use this procedure to reassign (add, replace or delete) the normal and alternate combined link set (CLS) and/or link sets (LSs) serving an existing destination point code (DPC). The new CLS/LSs being assigned to the DPC must already be provisioned.

This procedure includes special steps to handle the deletion and replacement of LSs that specify the target DPC as their adjacent point code (APC).

PROCEDURE

1. At an RC/V terminal, enter **16.10r** to access the SIGNALING POINT CODE view in REVIEW mode.

Specify the key fields associated with the target DPC:

POINT CODE	(9-digit DPC number)
GSM	(target GSM number)

Is the view displayed?

- If **no**, the target DPC is not defined on the target GSM, and this procedure is not appropriate; EXIT this procedure immediately. Use the procedure "Define New Destination Point Codes," Procedure 13.1.7, to define a *new* DPC, or choose a different DPC to be modified.
- If **yes**, all other fields on the form are populated with current values, and LS/CLS updates may occur; CONTINUE this procedure.

2. When this procedure is complete, will *both* CLS(s) and ordinary LS(s) be used as normal/alternate link sets?

- If **yes**, determine the constituent LSs associated with each intended CLS by issuing the input message:

OP:CCS,CLS,SET=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the identified CLS number and **xxx** is its GSM number. To this list, add all intended ordinary LSs.

If the list contains *any duplication*, EXIT this procedure immediately, because individual link sets assigned as routes to a DPC must be unique. Choose new CLS/LS candidates and re-enter this procedure.

If the list contains *no duplication*, CONTINUE this procedure.

- If **no**, CONTINUE this procedure.

3. Note the value of the ADJACENT field on the **16.10** view.

- If the field is **no**, the target DPC is *not* an APC; SKIP to Step 8.
- If the field is **yes**, the target DPC is an APC; CONTINUE this procedure.

4. Are any of the NORMAL LINK SET or ALTERNATE LINK SETS displayed on the **16.10** view a CLS, whose number is in the range 256-511?

— If **yes**, determine the constituent LSs, by issuing the input message:

OP:CCS,CLS,SET=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the identified CLS number and **xxx** is its GSM number, and then CONTINUE this procedure.

— If **no**, CONTINUE this procedure.

5. Create a list of LSs serving the target DPC, composed of ordinary LSs (in the range 1-255) in the NORMAL LINK SET or ALTERNATE LINK SETS fields displayed on the **16.10** view (if any), plus the LS components associated with the CLS derived in Step 4 (if any).

For **each** identified LS, display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on an MCC/STLWS, where **aaa** is the LS number and **xxx** is the GSM number. Does the **APC** (displayed on the 1533 page) of **any** of the LSs **match** the *target DPC*?

— If **yes**, CONTINUE this procedure.

— If **no**, SKIP to Step 8.

6. Are any of the LSs, identifying the target DPC as an APC, to be deleted or replaced by this procedure?

— If **yes**, CONTINUE this procedure.

— If **no**, SKIP to Step 8.

7. Display the **1532,xxx CCS LINK SET SUMMARY** page on the MCC/STLWS, where **xxx** is the target GSM number, and observe the status of the target LS. Is the status of the target LS in GROW (implying there are no child CCSLKs provisioned in the LS)?

— If **yes**, CONTINUE this procedure.

— If **no**, use the procedure "Delete Link Set Members," Procedure 13.1.15, to delete **all** child CCSLKs; then CONTINUE this procedure.

8. Is a CLS to be used as a *new* route to the DPC as a normal/alternate link set?

— If **yes**, CONTINUE this procedure.

— If **no**, SKIP to Step 10.

9. Determine if the new CLS to be used for DPC access is provisioned on the target GSM, by issuing the input message:

OP:CCS,CLS,SET=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the target CLS number and **xxx** is its GSM number.

- If the string *NO DATA FOUND* appears in the response, the specified CLS does **not** exist; EXIT this procedure immediately, and reexecute it, after using the procedure "Define a New Combined Link Set," Procedure 13.1.6, to define the CLS (or choose a new CLS/LS route).
 - Otherwise, CONTINUE this procedure.
10. If any *new* LSs are to be used as a DPC route, display the **1532,xxx CCS LINK SET SUMMARY** page on the MCC/STLWS, where **xxx** is the target GSM number, and observe the provisioned LSs displayed (the status of the LS is irrelevant). Search for the new LSs chosen for DPC routes.
- If **all** identified LS candidates appear (or **no** ordinary LSs are designated as new routes), CONTINUE this procedure.
 - If any of the LSs candidates are **not** displayed, EXIT this procedure immediately. Use the procedure "Define New Link Sets," Procedure 13.1.5, to add the missing LSs (or alter the choice of LS routes).
11. At an RC/V terminal, enter **16.10u** to access the SIGNALING POINT CODE view in UPDATE mode.

Specify the key fields:

POINT CODE	(target 9-digit DPC number)
GSM	(target GSM number)

All the other fields are populated with current values and the string *Enter Update, Change, Validate, or Print:* is produced.

12. Is this procedure being used to **delete** (not replace) the **NORMAL LINK SET** LS/CLS serving the target DPC?
- If **no**, CONTINUE this procedure.
 - If **yes**, and alternate routes exist, use Step 13 to replace the normal route with one of the alternate routes, and CONTINUE this procedure.
 - If **yes**, and no alternate routes exist, EXIT this procedure immediately, because a DPC is not allowed to exist without at least *one* CLS/LS route. Instead, use the procedures "Delete Destination Point Codes," Procedure 13.1.16, to delete the DPC from the GSM entirely.
13. Enter **c** to start change mode. The expected response is the *Change field:* string. Enter the **number of the field** to be updated to move the cursor to the field; for alternate link sets the response will ask for a row number before moving to that field.
- NORMAL LINK SET (or ALTERNATE LINK SETS 1/2/3/4)
- Enter the new LS or CLS value (this could be an addition or replacement); to "blank" a field (delete a LS/CLS), enter an ' (apostrophe). The expected response is the *Change field:* string.
14. Have all the required CLS/LSs been updated?
- If **yes**, CONTINUE this procedure.
 - If **no**, RETURN to Step 13 for the other CLS/LS modifications.

15. Enter < to return to the update command line and u to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu and q to exit RC/V.

16. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

17. All LSs (including those LSs identified as a member of the CLS), that were identified as being disassociated from their APC in Steps 5-7 of this procedure, should be deleted.

SKIP to the procedure "Delete Link Sets," Procedure 13.1.18 , to delete the identified LSs.

18. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.14: Modify Link Member Characteristics

OVERVIEW

Use this procedure to alter the characteristics of existing signaling links (CCSLKs).

Before entering this procedure, the following data should be available, per local procedures:

- If the PH termination is to be changed, the new termination must be an unassigned member of an existing CCS channel group, or a member of a CCS channel group not yet defined
- If the signaling data link (SDL) termination is to be changed, the new access termination on a DFI/DNU-S facility on the target GSM must correspond to an equipped, but unassigned port.
- Any change in the signaling link code (SLC) must be negotiated with the APC.

Some modifications require compatible link updates in the far-end APC exchange.

PROCEDURE

1. Verify the target CCSLK already exists on the GSM by displaying the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on an MCC/STLWS, where **aaa** is the parent LS number and **xxx** is its GSM number.

Is the page displayed, with the CCSLK to be updated being present?

- If **yes**, CONTINUE this procedure.
- If **no**, this procedure is not appropriate; EXIT this procedure immediately.

2. Is the target CCSLK in a deactivated (**DACT**) state?

- If **yes**, CONTINUE this procedure.
- If **no**, and you are updating congestion thresholds or transfer rate per 20ms fields, CONTINUE this procedure.
- If **no**, and you are updating other fields, execute the **2xx,UCL** menu command, where **xx** is the CCSLK member number, to deactivate the CCSLK; then CONTINUE this procedure.

3. Is the CCSLK PSU termination to be changed?

- If **yes** and the new termination is on a **new** PSU channel group, CONTINUE this procedure.
- If **yes**, and the new termination will be on an **existing** PSU channel group, SKIP to step 5.
- If **no**, SKIP to Step 6.

4. Use the procedure "Preparing the Packet Switch Unit for CCS Assignment," Procedure 13.1.8, to prepare the PSU environment for CCSLK provisioning (to establish hardware for a new channel group), and then CONTINUE this procedure at Step 6.

5. At an RC/V terminal, enter **16.11r** to access the CHANNEL GROUP ASSIGNMENT DEFINITION view in REVIEW mode.

Specify the key fields:

SM	(target GSM number)
SHELF	(target PSU shelf number)
CHGRP	(target channel group)

Is the view displayed?

- If **no**, EXIT this procedure immediately and re-evaluate the choice of PH termination.
- If **yes**, and if the proposed channel group member is **already assigned**, EXIT this procedure and re-evaluate the choice of PH termination.
- If **yes**, and the proposed channel group member is **not assigned**, CONTINUE this procedure.

6. Is the SDL termination to be changed?

- If **no**, SKIP to Step 9.
- If **yes**, and the new access uses a **DNU-S**, SKIP to Step 8.
- If **yes**, and the new access uses a **DFI/DFI2**, CONTINUE this procedure.

7. The new SDL is defined by its digital equipment number (DEN), which is composed of the following components:

DEN=a-b-c-d

where **a** is the target GSM number, **b** is the DLTU (digital line trunk unit) number, **c** is the DFI (digital facility interface) number, **d** is the DS0 channel number.

At an RC/V terminal, enter **7.41** to access the T1 CHANNEL USAGE view in REVIEW mode.

Specify the key fields:

SM	(target GSM number)
DLTU	(digital line trunk unit number)
DFI	(digital facility interface number)
FAC IND	(should be 0 for a DFI, 1 for DS0 channels in the range 1-24 on a DFI2, or 2 for channels in the range 25-48 on a DFI2)

Is the view displayed?

- If **no**, EXIT this procedure. Refer to the *PROCEDURE 3.25, Perform DFI/DFI-2 Growth* procedure in 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures - Growth* document to equip the appropriate hardware, or choose another SDL termination.
- If **yes**, and the proposed DS0 channel is **already assigned**; EXIT this procedure and choose another SDL termination.
- If **yes**, and the proposed DS0 channel is **not assigned**; SKIP to Step 9.

Enter < to return to the forms menu and **q** to exit RC/V.

8. The new SDL, defined by its network equipment number (NEN), has the following components in pre-5E13 software releases:

NEN=a-b-x-y-vv-c

where **a** is the target GSM, **b** is the digital network unit - SONET (DNU-S) number, **x** is the data group (DG), **y** is the synchronous transport signal (STS) number, **vv** is the virtual tributary 1.5 (VT1.5), and **c** is the DS0 channel number in the range 1-24.

For 5E13 and later software releases, the NEN definition is altered to redefine synchronous transport signal and virtual tributary numbering conventions to accommodate Bellcore standards, specifically:

NEN=a-b-x-s-y-g-m-c

where **s** is the SONET termination equipment (STE) number, **g** is the virtual tributary group (VTG) number, and **m** is the virtual tributary member (VTM) number.

At an RC/V terminal, enter **7.42** to access the DS1 CHANNEL USAGE view in REVIEW mode.

Specify the key fields from the proposed target SDL termination in pre-5E13 software releases:

SM	(target GSM number)
DNU-S	(digital network unit number)
DATA GROUP	(data group number)
STS	(synchronous transport signal number)
VT	(VT1.5 facility)

For 5E13 and later software releases, the key fields change to reflect new synchronous transport signal and virtual tributary numbering conventions, specifically:

SM	(target GSM number)
DNU-S	(digital network unit number)
DATA GROUP	(data group number)
STE	(SONET termination equipment number)
STS	(synchronous transport signal number)
VT GROUP	(virtual tributary group)
VT MEMBER	(virtual tributary member)

Is the view displayed?

- If **no**, EXIT this procedure. Refer to the *PROCEDURE 3.196, Perform DNU-S Service TMUX Pack Growth* procedure in 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures - Growth* document to equip the appropriate hardware, or choose another SDL termination.
- If **yes**, and the proposed DS0 channel is **already assigned**; EXIT this procedure immediately and choose another SDL termination.
- If **yes**, and the proposed DS0 channel is **not assigned**; CONTINUE this procedure.

Enter < to return to the forms menu and **q** to exit RC/V.

9. At an RC/V terminal, enter **16.6u** to access the SIGNALING LINK SET MEMBER view in UPDATE mode.

Specify the key fields:

LINK SET	(parent LS number)
MEMBER	(CCSLK member)

GSM	(target GSM number)

All the other fields are populated with current values and the string *Enter Update, Change, Validate, or Print:* is produced.

10. Enter **c** to start change mode. The expected response is the *Change field:* string. Enter the **number of the field** to be updated to move the cursor to the field and enter the new value.
11. Have all the required fields been updated?
 - If **yes**, CONTINUE this procedure.
 - If **no**, RETURN to Step 10 until all fields have been changed.

12. Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

A message

REPT CCS SM=xxx ODD BACKUP WARNING

(where **xxx** is the GSM number) warns you to backup the ODD promptly to avoid serious roll-forward problems, should the target GSM undergo an initialization. This message will be produced only if the SLC, access office equipment or PSU termination was updated.

Enter **<** to return to the forms menu and **q** to exit RC/V.

13. Back up the new ODD by entering the input message:

BKUP:ODD

on an MCC/STLWS.

14. Display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on the MCC/STLWS, where **aaa** is the LS number (parent of the modified CCSLK) and **xxx** is the target GSM.

The modified CCSLK will be present with current characteristics displayed. If the CCSLK is in a deactivated (**DACT**) state, then attempt to activate the CCSLK by entering **3xx**, where **xx** is the CCSLK member number.

If the CCSLK does not successfully restore, it may be that the far-end exchange has not yet completed its update procedure for the link. Investigate the failure using the procedures in "Problem Analysis Strategies," Procedure 14.1.

15. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.15: Delete Link Set Members

OVERVIEW

Use this procedure to delete individual or all existing signaling links (CCSLKs) in a link set (LS) from a specific GSM.

CAUTION: UNCONDITIONAL removals used in this procedure may impact CCS operation. If deleting the last member in a LS, it is possible that one/more signaling routes may become permanently inaccessible. As the only legitimate reason to take this latter action is to ultimately delete the parent LS, it is advisable to start at the procedure "Delete Link Sets," Procedure 13.1.18, which provides appropriate defensive checks against inadvertent actions.

Assume that compatible link deletion activities have occurred/will occur in the far-end APC exchange.

PROCEDURE

1. How many CCSLKs are being deleted?
 - If an **individual** CCSLK is being deleted, SKIP to Step 3.
 - If **all** members in a LS are to be deleted, CONTINUE this procedure.
2. Display the **1532,xxx CCS LINK SET SUMMARY** page on the MCC/STLWS, where **xxx** is the target GSM number.
 - If the LS to be deleted is **not** displayed or has **GROW** status, this procedure is not appropriate; EXIT this procedure immediately.
 - If the LS to be deleted is displayed, execute the **2xxx** menu command, where **xxx** is the target LS number, to **UNCONDITIONALLY** deactivate all CCSLKs in the LS. Authorize the deactivation when warned of the danger by MCC prompts, and then SKIP to Step 4.
3. Display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on the MCC/STLWS, where **aaa** is the parent LS number associated with the target CCSLK and **xxx** is its GSM number.
 - If the CCSLK to be deleted is displayed, **UNCONDITIONALLY** deactivate the CCSLK by executing the menu command **2xx,UCL**, where **xx** is the target CCSLK member number, and then CONTINUE this procedure.
 - If the target CCSLK to be deleted is **not** displayed, this procedure is not appropriate; EXIT this procedure immediately.
4. At an RC/V terminal, enter **16.6d** to access the SIGNALING LINK SET MEMBER view in DELETE mode.
5. Specify the key fields:

LINK SET	(parent LS number)
MEMBER	(target CCSLK member)
GSM	(target GSM number)

Only the key fields are displayed and the string *Enter Delete, Validate, or Print:* is produced.

6. Enter **d** to complete the deletion process. When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

A message

REPT CCS SM=xxx ODD BACKUP WARNING

(where **xxx** is the GSM number) warns you to backup the ODD promptly to avoid serious roll-forward problems, should the target GSM undergo an initialization.

7. Is this procedure being used to delete **all** CCSLKs in a LS, **and** are there still CCSLKs to be deleted?

— If **yes**, RETURN to Step 5 to delete another CCSLK.

— If **no**, CONTINUE this procedure.

8. Enter **<** to return to the forms menu and **q** to exit RC/V.

9. Display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on the MCC/STLWS, where **aaa** is the parent LS number associated with the target CCSLK and **xxx** is its GSM number.

Verify that the deleted CCSLKs are not displayed.

10. Back up the new ODD by entering the input message:

BKUP:ODD

on an MCC/STLWS.

11. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.16: Delete Destination Point Codes

OVERVIEW

This procedure deletes one or more existing destination point codes (DPCs) as signaling routes from a specific GSM. Special considerations are required, if the DPC is an adjacent point code (APC) which directly terminates a provisioned LS from the target GSM, or the DPC terminates a GSM trunk route.

PROCEDURE

1. At an RC/V terminal, enter **16.10r** to access the SIGNALING POINT CODE view in REVIEW mode.

Specify the key fields associated with the DPC to be deleted:

POINT CODE	(9-digit target DPC number)
GSM	(target GSM number)

Is the view displayed?

- If **no**, the target DPC does not exist; EXIT this procedure immediately.
- If **yes**, and the value of the ADJACENT field is **no**, the target DPC is not an APC; SKIP to Step 7.
- If **yes**, and the value of the ADJACENT field is **yes**, the target DPC is an APC; CONTINUE this procedure.

Enter < to return to the forms menu and **q** to exit RC/V.

2. Are any of the NORMAL LINK SET or ALTERNATE LINK SETS displayed on the **16.10** view a CLS with a number in the range 256-511?

- If **yes**, determine the constituent LSs, by issuing the input message:

OP:CCS,CLS,SET=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the identified CLS number and **xxx** is the target GSM number, then CONTINUE this procedure.

- Otherwise, CONTINUE this procedure.

3. Create a list of LSs serving the target DPC, composed of ordinary LSs, in the range 1-255, in the NORMAL LINK SET or ALTERNATE LINK SETS displayed on the **16.10** view (if any), plus the LS components associated with the CLS as determined in Step 2 (if any).

For **each** identified LS, display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on an MCC/STLWS, where **aaa** is the LS number and **xxx** is the target GSM number.

Does the **APC** (displayed on the 1533 page) of any LSs match the **target DPC**?

- If **yes**, CONTINUE this procedure.
- If **no**, SKIP to Step 7.

4. When the APC is deleted, any terminating LSs (identified in Step 3) will ultimately be deleted. Therefore, such LSs must not be used as routes to any other DPC.

Issue the input message:

OP:OFR,FORM=6006, DEVICE=xxx

on an MCC/STLWS, to produce office records for the SIGNALING POINT CODE view. The device **xxx** is described in "Signaling Link Provisioning Overview," Procedure 13.1.

Determine if **any other DPCs** (not the identified **APC**) on the target GSM are served by the target LS identified in Step 3.

For **each** DPC identified in the form output, use the procedure "Modify Link Sets Serving a DPC," Procedure 13.1.13, to update LS assignments, deleting the targeted LS as a route; then CONTINUE this procedure.

5. When the APC is deleted, any terminating LSs (identified in step 3) will ultimately be deleted. Therefore, such LSs must not be assigned to any combined link set (CLS).

Issue the input message:

OP:CCS,LSCLS,LS=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the target LS number identified in Step 3 and **xxx** is its GSM number.

If a CLS is identified, use the procedure "Delete Combined Link Sets," Procedure 13.1.17, to delete the CLS, or use the procedure "Redefine Combined Link Set Members," Procedure 13.1.12, to replace the target LS with a new one; then CONTINUE this procedure.

6. When the APC is deleted, all CCSLKs in the terminating LSs must also be deleted (as the LS itself will ultimately be deleted). Use the procedure "Delete Link Set Members," Procedure 13.1.18, to delete **all** member CCSLKs of the affected LSs (if any).

Before continuing to the next step, display the **1532,xxx CCS LINK SET SUMMARY** page on an MCC/STLWS, where **xxx** is the target GSM number, to verify **all** LSs, identifying the target DPC as their APC, are in the **GROW** state.

7. Issue the input message:

OP:SS7,OPC=aaa,DPC=bbb

on an MCC/STLWS, where **aaa** is the target GSM's OPC (identified on the 1532,xxx MCC page, where **xxx** is the target GSM) and **bbb** is the target DPC.

Are any trunk groups (TGs) identified in the output message, terminating on the target DPC?

— If **yes**, CONTINUE this procedure.

— If **no**, SKIP to Step 9.

8. One or more TGs, which originate on the target GSM and terminate on the target DPC, must be deleted before the DPC is deleted. Use the procedure "Delete Trunk Routes," Procedure 13.2.3, to delete the identified TGs, then CONTINUE this procedure.
9. Issue the input message:

OP : CCS , SCMG , SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM number.

Based on the output produced, do one of the following:

- If the DPC to be deleted by this procedure **is identified** in the output, CONTINUE this procedure.
- Otherwise, SKIP to Step 11.

10. A DPC cannot be deleted if it is provisioned as a primary or backup signaling connection control part (SCCP) route. Use procedure "Update Backup SCCP Route Destination," Procedure 13.3.9 , to alter the backup SCCP destination, or use "Delete Primary SCCP Route Destinations," Procedure 13.3.20 , to degrow primary/backup SCCP destinations.

Then, CONTINUE this procedure.

11. At an RC/V terminal, enter **16.10d** to access the SIGNALING POINT CODE view in DELETE mode.

Specify the key fields:

POINT CODE	(target DPC number)
GSM	(target GSM number)

Only the key fields are displayed and the string *Enter Delete, Validate, or Print:* is produced.

12. Enter **d** to complete the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

13. Verify that the DPC has been deleted.

Issue the input message:

OP : CCS , DPC , DPCID=aaa , SM=xxx

on an MCC/STLWS, where **aaa** is the 9-digit deleted DPC number and **xxx** is its GSM number. The string *INVALID DPC* should appear in the output.

14. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

15. Delete all LSs (including those LSs identified as a member of the CLS), that were identified in Step 3 as using the deleted DPC as an APC. Use the procedure "Delete Link Sets," Procedure 13.1.18 , to delete the identified LSs.
16. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.17: Delete Combined Link Sets

OVERVIEW

Use this procedure to undefine a combined link set (CLS) on a GSM.

PROCEDURE

1. To delete the CLS, it must already be defined on the GSM. Issue the input message:

OP:CCS,CLS,SET=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the target CLS number and **xxx** is its GSM.

- If the string *NO DATA FOUND* appears in the response, the target CLS is **not** currently defined on the target GSM, and this procedure is not appropriate; EXIT this procedure immediately.
- Otherwise, the target CLS exists; CONTINUE this procedure.

2. Issue the input message:

OP:OFR,FORM=6006,DEVICE=xxx

on an MCC/STLWS, to produce office records for the SIGNALING POINT CODE view. The device **xxx** is described in the "Signaling Link Provisioning Overview," Procedure 13.1.

Determine **all DPCs** on the target GSM that are served by the identified CLS.

For **each** DPC identified in the outputted form, use the procedure "Modify Link Sets Serving a DPC," Procedure 13.1.13, to update LS/CLS assignments, so that the targeted CLS is deleted as a route, and then CONTINUE this procedure.

3. At an RC/V terminal, enter **16.7d** to access the COMBINED SIGNALING LINK SET view in DELETE mode.

Specify the key fields:

CLS	(target combined link set number)
GSM	(target GSM number)

Only the key fields are displayed and the string *Enter Delete, Validate, or Print:* is produced.

4. Enter **d** to complete the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

5. To verify that the CLS has been deleted issue the input message:

OP:CCS,CLS,SET=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the target CLS number and **xxx** is its GSM number. The phrase *NO DATA FOUND* should appear in the response.

6. Back up the new ODD by entering the input message:
BKUP : ODD
on an MCC/STLWS.
7. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.18: Delete Link Sets

OVERVIEW

Use this procedure to delete an existing link set (LS) serving a GSM.

PROCEDURE

1. Display the **1532,xxx CCS LINK SET SUMMARY** page on the MCC/STLWS, where **xxx** is the target GSM number. and observe the status of the target LS. Is the status of the target LS in GROW (implying there are no member CCSLK provisioned in the LS)?
 - If **yes**, CONTINUE this procedure.
 - If the target LS is **not displayed**, the LS does not exist and this procedure is inappropriate; EXIT this procedure immediately.
 - Otherwise, use the procedure "Delete Link Set Members," Procedure 13.1.15 , to delete **all** member CCSLKs; then CONTINUE this procedure.

2. Issue the input message:

OP:OFR,FORM=6006, DEVICE=xxx

on an MCC/STLWS, to produce office records for the SIGNALING POINT CODE view. The device **xxx** is described in the "Signaling Link Provisioning Overview," Procedure 13.1 .

Determine if **any** DPCs on the target GSM are served by the specified link set (LS).

For **each** DPC identified in the output, use the procedure "Modify Link Sets Serving a DPC," Procedure 13.1.13 , to update LS/CLS assignments, deleting the targeted LS as a route; then CONTINUE this procedure.

3. Issue the input message:

OP:CCS,LSCLS,LS=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the target LS number and **xxx** is its number.

If a CLS is identified, use the procedure "Delete Combined Link Sets," Procedure 13.1.17 , to delete the CLS, or use the procedure "Redefine Combined Link Set Members," Procedure 13.1.12 , to replace the target LS with a new one; then CONTINUE this procedure.

4. At an RC/V terminal, enter **16.5d** to access the SIGNALING LINK SET view in DELETE mode.

Specify the key fields:

LINK SET	(target link set number)
GSM	(target GSM number)

Only the key fields are displayed and the string *Enter Delete, Validate, or Print:* is produced.

5. Enter **d** to complete the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu and q to exit RC/V.

6. Verify that the LS has been deleted by displaying the **1532,xxx CCS LINK SET SUMMARY** page on the MCC/STLWS, where **xxx** is the target GSM number.
7. Back up the new ODD by entering the input message:
BKUP:ODD
on an MCC/STLWS.
8. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.19: Delete Intra-SM Message Delivery Link

OVERVIEW

Use this procedure to delete the intra-SM MD link.

CAUTION: A successful deletion will stop all ISUP trunk/TCAP activity using a PSU platform on the parent GSM.

This procedure should only be performed in the following cases:

- To change the PSU termination (if absolutely necessary to improve reliability or throughput).
- To completely eliminate CCS functionality on a PSU platform from the GSM.

PROCEDURE

1. Determine the status of the intra-SM MD link by issuing the input message:

OP : STATUS , MD , SM=xxx

on an MCC/STLWS, where xxx is the target GSM.

- If the MD link is **unequipped** (failure reason **NONEXISTENT MD PATH** will appear in the output), this procedure is inappropriate; EXIT this procedure immediately.
- If the MD link status is **OOS-DEACTIVATED**, CONTINUE this procedure.
- Otherwise, issue the input message:

RMV : MD , SM=xxx , UCL

on an MCC/STLWS, where xxx is the target GSM number. Then CONTINUE this procedure.

2. At an RC/V terminal, enter **16.17d** to access the MESSAGE DELIVERY LINK view in DELETE mode.

Specify the key field:

SM	(target GSM number)

Only the key field is displayed and the string *Enter Delete, Validate, or Print:* is produced.

3. Enter **d** to complete the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

A message

REPT CCS SM=xxx ODD BACKUP WARNING

(where xxx is the GSM number) warns you to backup the ODD promptly to avoid serious roll-forward problems, should the target GSM undergo an initialization.

Enter **<** to return to the forms menu and **q** to exit RC/V.

4. Verify that the intra-SM MD has been deleted by displaying the **1530,xxx MESSAGE DELIVERY LINK** page on the MCC/STLWS, where **xxx** is the target GSM number, and observe that the status is *UNEQ* (unequipped).
5. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.
6. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.20: Undefine CCS Global Switching Module Existence

OVERVIEW

This procedure undefines a global SM (GSM) and deletes all its corresponding CCS signaling functionality.

PROCEDURE

1. Display the **1532,xxx CCS LINK SET SUMMARY** page on the MCC/STLWS, where **xxx** is the target GSM number, and check for the existence of LSs (link sets). Are any LSs displayed (regardless of state)?
 - If **no**, CONTINUE this procedure.
 - If **yes**, **delete all** displayed LSs, using the procedure "Delete Link Sets," Procedure 13.1.18, and then CONTINUE this procedure.
 2. Display the page **1530,xxx MESSAGE DELIVERY LINK** on the MCC/STLWS, where **xxx** is the target GSM number, and check the existence of the intra-SM MD link status.
 - If **UNEQ** (unequipped) status is displayed, no intra-SM MD link exists on the target GSM; CONTINUE this procedure.
 - If other status/equipment information **is** displayed, the intra-SM MD link exists and the GSM may not be undefined; EXIT this procedure immediately.

Use the procedure "Delete Intra-SM Message Delivery Link," Procedure 13.1.19, to delete the intra-SM MD link, and then RESTART this procedure.
 3. At an RC/V terminal, enter **16.20r** to access the SCCP NETWORKS DEFINITION view in REVIEW mode.
- Specify the key field:

GSM	(target GSM to be deleted)

Is the view displayed?

- If the response "FORM NOT FOUND" is produced, CONTINUE this procedure.
- If the view is displayed, the GSM to be deleted has been designated as an **SCCP GSM**. Use the procedure "Delete Connectionless SCCP GSM," Procedure 13.3.22, to completely deactivate SCCP processing on the target GSM, and then CONTINUE to the next step.

Enter < to return to the forms menu.

4. At an RC/V terminal, enter **16.1d** to access the GLOBAL SM view in DELETE mode. Specify the key field:

GSM	(target GSM number)

Only the key field is displayed and the string *Enter Delete, Validate, or Print:* is produced.

5. Enter **d** to complete the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen

Enter < to return to the forms menu and q to exit RC/V. Before continuing wait for this message:

```
CFR SPRMEM IMAGE=SPAREMEM SM=x TYPE=DEGROW COMPLETED  
MEMORY POINTERS UPDATED - ODD BACKUP REQUIRED
```

NOTE: It may take some time before this message appears, depending upon SM occupancy.

6. Verify the GSM has been deleted by trying to display the **1532,xxx CCS LINK SET SUMMARY** page on the MCC/STLWS, where **xxx** is the target GSM number. The page should **not** display.
7. Back up the new ODD by entering the input message:

BKUP:ODD

on an MCC/STLWS.

8. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.21: Provisioning of 5E13 Maintenance Enhancements

OVERVIEW

This procedure allows administrators to activate or deactivate enhanced maintenance features on all global SMs. These features (available in 5E13 and later software releases) are:

- False link congestion is a condition where a CCSLK remains in service, but is effectively transmitting few or no messages. If a link stays at the same congestion level for a long period of time despite traffic throttles, it is likely that the congestion is probably due to a more severe root cause than traffic load.

Elimination of false link congestion is accomplished by a complete restart of the CCSLK, if that link remains in the same congestion level for long periods of time (user-defined by recent change) despite applied throttles. Elimination of false link congestion at levels 2 and 3 is in effect by default in 5E13 and later software releases, but the lesser impacting level 1 congestion control can be activated or deactivated by this procedure.

- A signaling link test (SLT) on a CCSLK guarantees reliable message transfer between the GSM and its APC. Such MTP level 3 test procedures are executed before a CCSLK is considered successfully restored, and periodically thereafter, on all active, noncongested CCSLKs (in all software releases supporting PSU signaling platforms).

In the 5E13 and later software releases, it is possible to activate a secured feature which allows periodic SLTs to be spawned even on congested links. This procedure provides the necessary provisioning sequence.

PROCEDURE

- Is the ability to eliminate false link congestion (congestion level 1) to be updated?
 - If **yes**, CONTINUE this procedure.
 - If **no**, SKIP to Step 4.
- At an RC/V terminal, enter **8.15u** to access the CCS OFFICE PARAMETER view in UPDATE mode.

Specify the key field:

OFFICE ID	(alphanumeric office identifier)

All the other fields are populated with current values and the string *Enter Update, Change, Validate, or Print:* is produced.

- Enter **c** to start change mode. The expected response is the *Change field:* string. Enter the **number** of the FLCONG LVL 1 field to move the cursor to that field (this field is only present in 5E13 and later software releases).

Enter **y** to *enable* detection of level 1 false link congestion, or **n** to *disable* this feature.

Enter **<** to return to the update command line and **u** to complete the update. When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

4. Is the improved SLT procedure for congested CCSLKs to be enabled or disabled?
 - If **yes**, and the secured improved SLT feature is **not activated**, CONTINUE this procedure.
 - If **yes**, and the secured improved SLT feature is **already activated**, SKIP to Step 7.
 - If none of the above, SKIP to Step 9.
5. Obtain a **password** for the Improved SLT feature (feature ID 176) from the Lucent Technologies Secured Feature Administrator.

Enter **8.22u** on an RC/V terminal to access the SECURED FEATURE UPGRADE view in UPDATE mode.

Specify the key fields:

FEATURE ID	(enter 176)
MODULE	(enter OFC for entire office)

The following pertinent fields are populated:

PASSWD	(blank)
ACTIVE	(populated with N for not active)
FEATURE NAME	(populated with IMPROVED SLT)

The string *Enter Update, Change, Validate, or Print:* is produced.

6. Enter **c** (for change mode), and enter the number of the PASSWD field; enter the password supplied by the administrator. Enter the number of the ACTIVE field, and populate with **Y** to activate the feature.

Enter **<** to return to the update command line, and **u** to complete the update. When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen. Enter **<** to return to the forms menu, and **q** to quit RC/V.

7. At an RC/V terminal, enter **8.15u** to access the CCS OFFICE PARAMETER view in UPDATE mode.

Specify the key field:

OFFICE ID	(alphanumeric office identifier)

All the other fields are populated with current values and the string *Enter Update, Change, Validate, or Print:* is produced.

8. Enter **c** to start change mode. The expected response is the *Change Field:* string. Enter the **number** of the IMPROVED SLT field to move the cursor to that field (although the field appears in pre-5E13 releases for CNI use, it has no impact on GSM PSU signaling platforms until 5E13).

Enter **y** to enable improved SLT operation on congested links, or **n** to disable this functionality.

Enter **<** to return to the update command line and **u** to complete the update. When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

9. Back up the new ODD by entering the message

BKUP : ODD

on an MCC or TLWS.

10. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.1.22: Operation, Maintenance and Administration Part Provisioning

OVERVIEW

This procedure allows updates to parameters associated with operation, maintenance and administration part (OMAP) procedures provided by the GSM in 5E13 and later software releases.

This includes MTP routing verification test (MRVT) and SCCP routing verification test (SRVT) functionality. See Section 12.5.3 for a detailed description of these administrative tools.

PROCEDURE

- At an RC/V terminal, enter **16.4u** to access the OMAP ROUTE VERIFICATION TEST TIMER PARAMETERS view in UPDATE mode.

Specify the key field:

GSM	(target GSM number)

The following fields will be populated with current data:

MRVT LOCAL	(maximum number of locally originated MRVTs)
MRVT ACK GUARD	(MRVT acknowledgment timer)
SRVT LOCAL	(maximum number of locally originated SRVTs)
SRVT ACK GUARD	(SRVT acknowledgment timer)

and the string *Enter Update, Change, Validate, or Print:* is produced.

- Enter **c** to start change mode. The expected response is the *Change Field:* string. Enter the **number** of the field to be updated to move the cursor to that field.

Enter new values for the desired OMAP timers/parameters based on the values listed in Table 13.1.22-1.

Table 13.1.22-1 OMAP Timer/Parameter Ranges

Timer/Parameter Field	Range	Default
MRVT LOCAL	1-5	5
MRVT ACK GUARD	8-15 (sec)	8 (sec)
SRVT LOCAL	1-5	5
SRVT ACK GUARD	8-15 (sec)	8 (sec)

Continue entering new field numbers and timer/parameter values until all identified fields are changed.

- Enter **<** to return to the update command line and **u** to complete the update. When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

- Back up the new ODD by entering the message

BKUP : ODD

on an MCC or TLWS.

- STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.2: TRUNK ROUTE PROVISIONING

OVERVIEW

This section describes the provisioning procedures required to add, maintain, and delete ISUP trunking capabilities on a GSM, or to convert existing CNI-controlled ISUP trunks to become associated with a PSU platform on a GSM.

See Table 13.2-1 for a list of the RC/V views involved.

Table 13.2-1 ISUP Trunking RC/V Views

VIEW	TITLE	USE	PURPOSE
5.1	TRUNK GROUP	rid	Define ISUP trunk group characteristics
5.5	TRUNK MEMBER	rid	Define ISUP trunk member characteristics
5.10	COPY MEMBER TRUNK	i	Copy existing ISUP trunk characteristics, while defining other members of a trunk group
7.41	T1 CHANNEL USAGE	r	Review T1 channel usage on a DFI facility
7.42	DS1 CHANNEL USAGE	r	Review DS1 channel usage on a DNU-S facility
Note: The USE column indicates how the view is used: r for REVIEW, i for INSERT, u for UPDATE, and d for DELETE.			

Define new ISUP trunk routes using the procedures listed in Table 13.2-2, in the order listed.

Table 13.2-2 Install Trunk Routes from a GSM

JOB DESCRIPTION	PROCEDURE
Define new ISUP TGs	Procedure 13.2.1
Define new ISUP trunks	Procedure 13.2.2

The procedures listed in Table 13.2-3 are used for common provisioning activities such as changing ISUP trunk routes/trunk members, or associated characteristics.

Table 13.2-3 Typical ISUP Trunk Provisioning Activities

JOB DESCRIPTION	PROCEDURE
Define new ISUP TGs	Procedure 13.2.1
Delete obsolete ISUP TGs	Procedure 13.2.3
Define new ISUP trunks	Procedure 13.2.2
Delete obsolete ISUP trunks	Procedure 13.2.4

The procedures listed in Table 13.2-4 are used, in the order listed, to delete ISUP trunk routes, when a GSM (with CCS functionality on a PSU platform) no longer provides CCS access.

Table 13.2-4 Deleting All ISUP Trunk Routes on a GSM

JOB DESCRIPTION	PROCEDURE
Delete all ISUP trunks	Procedure 13.2.4
Delete all ISUP TGs	Procedure 13.2.3

The procedures listed in Table 13.2-5 are used in 5ESS®-2000 switch offices with both CNI and PSU platforms available to convert CNI-controlled ISUP trunks or multi-frequency (MF) trunks to become ISUP trunks associated with a GSM's PSU-based signaling platform (beginning with the 5E12 software release).

Table 13.2-5 Converting Existing Trunks to GSM Signaling Platform

JOB DESCRIPTION	PROCEDURE
Convert existing trunks to GSM signaling	Procedure 13.2.5
Convert existing trunk groups preserving route indices	Procedure 13.2.6

The remainder of this section provides the specific procedures to define, maintain, or delete ISUP trunking vehicles

on a GSM.

The procedures provide no information about the selection of values to be negotiated with regional CCS management, such as trunk types, or origination or destination point codes.

All of the procedures require access to RC/V views. This is accomplished by the choice of **196** menu selection, or the input message `rcv:menu:apprc` on an MCC/STLWS. Alternately, the input message `apprc` can be used on a *UNIX*[®]/RC terminal.

Some of the procedures that follow require specific **office records** be interrogated. In those procedures, an input command of the form

```
OP:OFR, FORM=###, DEVICE=xxx
```

will be specified. If **xxx** is "FILE", the office records will be deposited in a file `/rclog/OFR.Oy`, where **y** is the **REQUEST ID** in the command response; the file can be interrogated or printed according to local procedures. Alternately, if **xxx** is specified as "ttyR", output is produced directly on the resident office records printer (if available); other output destinations are possible, as defined on the `OP-OFR` input manual page in 235-600-700, *Input Messages Manual*.

The **8.15**, CCS OFFICE PARAMETERS view can be used in update mode, to adjust timers used for ISUP trunk maintenance/call processing signaling flow. These parameters apply to *all* ISUP trunks in 5ESS[®]-2000 switch offices when both CNI and PSU platforms are provisioned.

Consult local practices and 235-118-2xx, *Recent Change Reference* or 235-080-100, *5ESS[®]-2000 Switch Translation Guide (TG-5)* for detailed descriptions of RC/V fields.

The trunk route provisioning procedures in this section are:

PROCEDURE

1. Procedure 13.2.1 - Add New ISUP Trunk Routes
2. Procedure 13.2.2 - Add New ISUP Trunk Members
3. Procedure 13.2.3 - Delete Trunk Routes
4. Procedure 13.2.4 - Delete Trunk Members
5. Procedure 13.2.5 - Convert Existing Trunk Members
6. Procedure 13.2.6 - Convert Existing Trunk Routes

Procedure 13.2.1: Add New ISUP Trunk Routes

OVERVIEW

A trunk route or trunk group (TG) must be assigned specifically for GSM signaling. This procedure adds such an integrated services user part (ISUP) TG.

This procedure only assigns a **new** ISUP TG. To convert existing multi-frequency signaling (MF) TGs or CNI ISUP TGs to become GSM-based, use the procedure "Convert Existing Trunk Routes," Procedure 13.2.6.

This procedure uses the 5.1, TRUNK GROUP view, which contains multiple screens. This procedure does not describe all the screens and fields, but only highlights those items that are unique to GSM signaling.

PROCEDURE

1. To define a new ISUP TG, the origination point code (OPC) must be known, that is, the global SM (GSM) must be defined. Issue the input message:

OP : CCS , GSM , SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM number.

- If the command fails, the response is "NG - GSM MISMATCH" or "NG - NO GLOBAL SM IN OFFICE," the GSM has not yet been defined; EXIT this procedure immediately.
- Otherwise, the GSM is defined; CONTINUE this procedure.

2. To define a new ISUP TG, the target destination point code (DPC) must be defined for the target GSM.

Issue the input message:

OP : CCS , DPC , DPCID=aaa , SM=xxx

on an MCC/STLWS, where **aaa** is the 9-digit target DPC number and **xxx** is its GSM number.

- If the response contains the string **INVALID DPC**, the target DPC has **not** been defined for the GSM. This procedure is not appropriate; EXIT this procedure immediately.
- Otherwise, the DPC is defined (accessibility is irrelevant at this point); CONTINUE this procedure.

3. At an RC/V terminal, enter **5.1i** to access the TRUNK GROUP view in INSERT mode.

Enter the following data for the new TG:

TGN	(TG number)
MODULE	(0 to indicate global call routing, or the target GSM number to indicate local call routing)
ORIG PT CODE	(9-digit OPC associated with GSM)
DEST PT CODE	(9-digit target DPC to terminate TG)

noting that the GSM number must be entered in the MODULE field in 5ESS®-2000 switch VCDX offices, as only local routing is allowed.

Enter other fields on multiple screens as defined in the 235-080-100, 5ESS®-2000 Switch Translation Guide

(TG-5), which are negotiated for the local/far-end exchanges. When all data is entered, the string *Enter Insert, Validate, screen#, or Print:* is produced.

4. Enter **i** to complete the insert.

When the insertion completes, "FORM INSERTED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

5. Issue the input message:

OP:OFR,FORM=5303,DEVICE=xxx

on an MCC/STLWS, to produce office records for the ROUTE INDEX (ROUTING) view. The device **xxx** is described in "Trunk Route Provisioning Overview," Procedure 13.2.

Determine **all existing route indexes** in the office. Decide if only **existing** route indexes are to be assigned to the new TG. Also, determine the numbers and characteristics of **new** route indexes, and alternate route designation updates caused by the introduction of the new TG, according to local practices.

6. Determine the action to be taken from the following list:

- If a **new** route index is to be defined, CONTINUE with Step 7.
- If an **existing** route index is to now reference the **new** TG, SKIP to Step 9.
- If any characteristic of a provisioned route index is to be **changed** (such as alternate routes), SKIP to Step 9.

7. At an RC/V terminal, enter **10.2i** to access the ROUTE INDEX (ROUTING) view in INSERT mode.

Enter the following data for the new route index:

RTI	(new route index)
ETYP	(route type)
TGN	(newly defined TG number)
NEXT RTI	(alternate route index)

Enter other fields as defined in the 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)*, as determined by local practices. When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

8. Enter **i** to complete the insert.

When the insertion completes, "FORM INSERTED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu (if no more route indexes are to be inserted), and **q** to quit RC/V (if no more route indexes are to be updated). SKIP to Step 11.

9. At an RC/V terminal, enter **10.2u** to access the ROUTE INDEX (ROUTING) view in UPDATE mode.

Specify the key field:

RTI	(route index to be updated)

All other fields are populated with current values, and the string *Enter Update, Change, Validate, or Print:* is produced.

10. Enter **c** to start change mode. The expected response is the *Change field:* string. Enter the **number of the field** to be updated to move the cursor to that field. Enter the new field value, and repeat for other fields as necessary.

When all changes have been made, enter **<** to return to the command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu (if no updates to other route indexes are to be made) and **q** to quit RC/V (if no further route indexes are to be inserted).

11. Have all new route indexes been inserted and all route index updates been completed?

— If **yes**, CONTINUE this procedure.

— If **no**, RETURN to Step 6.

12. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

13. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.2.2: Add New ISUP Trunk Members

OVERVIEW

This procedure adds *new* integrated services user part (ISUP) trunks to an existing trunk group (TG) associated with a GSM's OPC.

This procedure assigns one or more new ISUP trunks, specifically:

- A **single** trunk, with any valid set of characteristics.
- **Multiple** trunks,
 - with contiguous member numbers in the same TG,
 - with contiguous CLCI numbers,
 - with contiguous office equipment (OE) numbers of the same equipment type (TEN, DEN or NEN),
 - all other characteristics being the same.
- **One or more** trunks, with characteristics identical to an existing ISUP trunk, except
 - with a different member number in the same TG,
 - with a different CLCI code,
 - with different OE numbers of the same type.

If existing multi-frequency signaling (MF) trunks or CNI ISUP trunks are to become GSM-based, see the procedure "Convert Existing Trunk Members," Procedure 13.2.5.

This procedure uses the 5.5 TRUNK MEMBER RC/V view, which contains multiple screens. This procedure will not describe all the screens and fields, but will highlight facets that are unique to a GSM. Consult local practices and 235-118-2xx, *Recent Change Reference* or 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)* for details.

Before starting this procedure, an unassigned but equipped access termination should be identified. Before the new trunk can be used for call processing, equivalent provisioning must take place in the far-end exchange.

PROCEDURE

1. The ISUP trunk/trunks to be provisioned must be unique. Issue the input message:

OP:LIST,TG=xx

on an MCC/STLWS, where **xx** is the target TG.

- If **one/more** of the target ISUP trunks are already provisioned, this procedure is not appropriate; EXIT this procedure immediately. Reenter, after selecting different and unique trunks.
- Otherwise, the new ISUP trunks are unique; CONTINUE this procedure.

2. What is the access equipment type associated with the target ISUP trunks?

- If access is on an analog **trunk unit (TU)**, CONTINUE this procedure.
- If access is on a **digital facility interface (DFI)**, SKIP to Step 4.
- If access is on an analog **digital networking unit - SONET (DNU-S)**, SKIP to Step 5.

3. The **trunk equipment number (TEN)** port is composed of the following components:

TEN=a-b-c-d-e

where **a** is the GSM number, **b** is the trunk unit (TU) number, **c** is the service group (SG), **d** is the channel board (CHBD), and **e** is the TEN circuit number. The TEN selected **must** reside on the target GSM.

Enter

105Y,X (or **106Y,X**)

on an MCC/STLWS, to access TU status for service group SG 0 or 1, respectively, where **X** is the GSM number and **Y** is the TU number. Observe if the TEN circuits to be used for trunk assignment are displayed (implying they are equipped), noting the actual hardware status is irrelevant; the status block number of interest on the MCC display uses the CHBD as the "tens digit" and the TEN circuit number as the "units digit."

For **each** of the proposed target TEN ports, issue the input message:

OP:STATUS, TEN=a-b-c-d-e

where **a, b, c, d, e** are the target TEN port number previously noted. If **no** status is produced, the TEN port is unassigned.

Are **all** of the target **TEN** circuits equipped, and the corresponding ports unassigned?

- If **yes**, SKIP to Step 6.
- If **no**, EXIT this procedure immediately. Refer to the *PROCEDURE 3.45, Trunk Circuit Pack Growth* procedure in 235-105-231, *Hardware Change Procedures - Growth* to grow new TU hardware (or choose a new trunk termination).

4. The **digital equipment number (DEN)** is composed of the following components:

DEN=a-b-c-d

where **a** is the GSM number, **b** is the digital line trunk unit (DLTU) number, **c** is the digital facility interface (DFI) number, and **d** is the DS0 channel number. The DEN selected **must** reside on the target GSM.

At an RC/V terminal, enter **7.41** to access the T1 CHANNEL USAGE view in REVIEW mode.

Specify the key fields from the proposed target ISUP trunk terminations:

SM	(target GSM number)
DLTU	(digital line trunk unit number)

DFI	(digital facility interface number)
FAC IND	(should be 0 for a 24-channel DFI, 1 for DS0 channels in the range 1-24 on a DFI2, or 2 for channels in the range 25-48 on a DFI2)

Is the view is displayed?

- If **no**, EXIT this procedure and refer to *PROCEDURE 3.25, Perform DFI/DFI-2 Growth* in 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures - Growth* to grow a new DFI hardware (or choose a trunk termination).
- If **yes**, and the proposed DS0 channel is **already assigned**, EXIT this procedure and choose another trunk termination.
- If **yes**, and the proposed DS0 channel is **not assigned**, CONTINUE this procedure.

Enter < to return to the forms menu and q to exit RC/V.

5. The **network equipment number (NEN)** contains the following components in pre-5E13 software releases:

NEN=a-b-x-y-vv-c

where **a** is the GSM number, **b** is the digital network unit - SONET (DNU-S) number, **x** is the data group (DG), **y** is the synchronous transport signal (STS) number, **vv** is the virtual tributary 1.5 (VT1.5), and **c** is the DS0 channel number in the range 1-24. The NEN selected **must** reside on the target GSM.

For 5E13 and later software releases, the NEN definition is altered to redefine synchronous transport signal and virtual tributary numbering conventions to accommodate Bellcore standards, specifically:

NEN=a-b-x-s-y-g-m-c

where **s** is the SONET termination equipment (STE) number, **g** is the virtual tributary group (VTG) number, and **m** is the virtual tributary member (VTM) number.

At an RC/V terminal, enter **7.42** to access the DS1 CHANNEL USAGE view in REVIEW mode.

Specify the key fields from the proposed target ISUP trunk terminations in pre-5E13 software releases:

SM	(target GSM number)
DNU-S	(digital network unit number)
DATA GROUP	(data group number)
STS	(synchronous transport signal number)
VT	(VT1.5 facility)

For 5E13 and later software releases, the key fields have changed to reflect new synchronous transport signal and virtual tributary numbering conventions, specifically:

SM	(target GSM number)
DNU-S	(digital network unit number)
DATA GROUP	(data group number)
STE	(SONET termination equipment number)
STS	(synchronous transport signal number)
VT GROUP	(virtual tributary group)
VT MEMBER	(virtual tributary member)

Is the view displayed?

- If **no**, EXIT this procedure and refer to *PROCEDURE 3.196, Perform DNU-S Service TMUX Pack Growth* in 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures - Growth*, to grow a new

DNU-S facility or choose a new trunk termination.

- If **yes**, and the proposed DS0 channel is **already assigned**, EXIT this procedure and choose another trunk termination.
- If **yes**, and the proposed DS0 channel is **not assigned**; CONTINUE this procedure.

Enter < to return to the forms menu and **q** to exit RC/V.

6. Is this procedure being used to provision single or multiple ISUP trunks?

- If a **single** trunk is being provisioned, CONTINUE this procedure.
- If **multiple** trunks are being provisioned, with contiguous office equipment (OE) numbers, all of the same type (TEN, DEN or NEN), contiguous TG member numbers in the same TG, contiguous CLCI code, and all other characteristics being the same, SKIP to Step 8.
- If **multiple** trunks are to be provisioned, with the same OE type (TEN, DEN or NEN), members in the same TG, and all characteristics, other than the member, OE and CLCI code being the same as an existing trunk, SKIP to Step 9.

7. At an RC/V terminal, enter **5.5i** to access the TRUNK MEMBER view in INSERT mode.

Enter the following data for the new ISUP trunk:

TGN	(TG number)
MEMB NBR	(TG member number)
OE	(office equipment number - possible values follow)
CLCI TRK ID	(CLCI code)

The **OE** entries are:

- For a TEN, enter **T**, followed by TEN identifiers
- For a DEN, enter **D**, followed by DEN identifiers
- For a NEN, enter **N**, followed by NEN identifiers

Enter other fields on multiple screens as defined in the 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)* which are negotiated for the local/far-end exchanges. When all data is entered, the string *Enter Insert, Validate, screen#, or Print:* is produced.

SKIP to Step 10.

8. At an RC/V terminal, enter **5.5i** to access the TRUNK MEMBER view in INSERT mode.

Enter the following data for multiple ISUP trunks:

TGN	(TG number)
MEMB NBR	(the first target TG member number)
QTY	(the number of trunks to be inserted)
OE	(office equipment number of the first target trunk)
CLCI TRK ID	(CLCI code for the first target trunk)

The **OE** entries are:

- For a TEN, enter **T**, followed by TEN identifiers
- For a DEN, enter **D**, followed by DEN identifiers
- For a NEN, enter **N**, followed by NEN identifiers

Enter other fields on multiple screens as defined in the 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)* which are negotiated for the local/far-end exchanges. When all data is entered, the string *Enter Insert, Validate, screen#, or Print:* is produced.

SKIP to Step 10.

9. At an RC/V terminal, enter **5.10i** to access the TRUNK MEMBER COPY view in INSERT mode.

Enter the following data for the **existing** "source" ISUP trunk, which is to be copied:

SRC TGN	(TG number of the source trunk)
SRC MEM	(the source TG member number)

Enter the **DESTTRUNK** area, and enter data for **each new** ISUP trunk (up to 16 trunks can be defined), specifically:

MEM	(new TG member number)
OE	(new office equipment number)
CLCI TRK ID	(new CLCI code)

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

SKIP to Step 10.

10. Enter **i** to complete the insert.

When the insertion completes, "FORM INSERTED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

11. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

12. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.2.3: Delete Trunk Routes

OVERVIEW

This procedure deletes any trunk group (TG). Office administration may require deletion of an ISUP trunk route (or TG) on a GSM due to traffic considerations, or the removal of a DPC from GSM access.

PROCEDURE

1. Issue the input message:

OP:SS7,TG=xx

on an MCC/STLWS, where **xx** is the target TG, and check the existence of provisioned TG members.

- If the response is **TG INVALID**, the target TG does not exist and this procedure is not appropriate; EXIT this procedure immediately.
- If the response is **NO DATA FOUND**, the TG exists but contains no provisioned members; CONTINUE this procedure.
- If provisioned TG members **are** listed, these members must be deleted before continuing. Use the procedure "Delete Trunk Members," Procedure 13.2.4, to delete the identified trunk members, and then CONTINUE this procedure.

2. Issue the input message:

OP:OFR,FORM=5303,DEVICE=xxx

on an MCC/STLWS, to produce office records for the ROUTE INDEX (ROUTING) view. The device **xxx** is described in "Trunk Route Provisioning Overview," Procedure 13.2.

Determine **all existing route indexes** that reference the **TG to be deleted**. Decide whether these route indexes are to be assigned to a new trunk group, or be deleted entirely.

3. Determine the action to be taken from the following list, for each identified route index:

- If a specific route index is to be **deleted**, CONTINUE with Step 4.
- If a specific route index is to be assigned to **another TG**, SKIP to Step 6.

4. At an RC/V terminal, enter **10.2d** to access the ROUTE INDEX (ROUTING) view in DELETE mode.

Specify the key field:

RTI	(route index to be deleted)

Only the key field is displayed and the string *Enter Delete, Validate, or Print:* is produced.

5. Enter **d** to complete the deletion.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu (if no more route indexes are to be deleted), and **q** to quit RC/V (if no more route indexes are to be updated).

SKIP to Step 8.

6. At an RC/V terminal, enter **10.2u** to access the ROUTE INDEX (ROUTING) view in UPDATE mode.

Specify the key field:

RTI	(route index to be updated)

All other fields are populated with current values, and the string *Enter Update, Change, Validate, or Print:* is produced.

7. Enter **c** to start change mode. The expected response is the *Change field:* string. Enter the **number of the field** to be updated to move the cursor to that field; likely candidates are TGN (to assign a new TG to the route index) or NEXT RTI (to choose a new alternate route index).

When all changes have been made, enter < to return to the command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu (if no updates to other route indexes are to be made) and **q** to quit RC/V (if no further route indexes are to be deleted).

8. Have all route indexes associated with the target TG been deleted or updated?

— If **yes**, CONTINUE this procedure.

— If **no**, RETURN to Step 3.

9. At an RC/V terminal, enter **5.1d** to access the TRUNK GROUP view in DELETE mode.

Specify the TGN key field **or** unique pair TRUNK CHAR/FEND CLLI key fields to identify the trunk group to be deleted.

TGN	(target TG number)
TRUNK CHAR	(TG common language circuit identifier)
FEND CLLI	(far-end common language location identifier)

Only the key fields are displayed and the string *Enter Delete, Validate, or Print:* is produced.

10. Enter **d** to complete the deletion.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu and **q** to exit RC/V.

11. Back up the new ODD by entering the input message:

BKUP:ODD

on an MCC/STLWS.

12. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.2.4: Delete Trunk Members

OVERVIEW

This procedure deletes a single trunk member, or up to 24 trunks simultaneously. **Multiple** trunk deletions described in this procedure must satisfy the following criteria: **they must have contiguous member numbers in the same TG, continuous CLCI numbers, and contiguous office equipment numbers of the same type (TEN, DEN or NEN)**. Otherwise, multiple trunk deletions must be treated as a series of individual trunk actions.

Deletion of ISUP trunks on a GSM may be required due to traffic considerations, or the removal of a DPC from GSM access.

PROCEDURE

1. Issue the input message:

OP:SS7,TG=a

on an MCC/STLWS, where **a** is the target TG and check for the existence of provisioned TG members.

- If **any target ISUP trunks do not exist**, this procedure is not appropriate; EXIT this procedure immediately. Reenter the procedure when a valid set of trunks is determined.
- If **all target ISUP trunks are listed**, CONTINUE this procedure.

2. Before attempting to delete an ISUP trunk/group of trunks, remove the target trunks to a stable OOS state. Issue one of the following messages on an MCC/STLWS: either

RMV:TRK,TKGMN=a-b,OOS,CADN,DSBLD

for a single trunk deletion, or

RMV:TRK,TKGMN=a-c&&d,OOS,CADN,DSBLD

for a multiple trunk deletion, with contiguous member numbers in a TG.

In these messages, **a** is the TG number, **b** is a single trunk member, and **c** and **d** are the trunk member endpoints in a range of trunks.

It is possible that one or more trunk removals may fail (despite generous camp-on intervals). If so, reexecute these commands with an unconditional (UCL) option added, before continuing with the next step.

3. Is a single trunk or multiple trunks (with criteria previously described) being deleted by this procedure?
 - If a **single** trunk is being deleted, CONTINUE this procedure.
 - If **multiple** trunks are being deleted, SKIP to Step 5.

4. At an RC/V terminal, enter **5.5d** to access the TRUNK MEMBER view in DELETE mode.

Specify the key fields:

TGN	(target TG number)

MEMB NBR	(target member number)

Only the key fields are displayed and the string *Enter Delete, Validate, or Print:* is produced.

Repeat this step for each member being deleted, then SKIP to Step 6.

5. At an RC/V terminal, enter **5.5d** to access the TRUNK MEMBER view in DELETE mode.

Specify the key fields:

TGN	(target TG number)
MEMB NBR	(member number of the first trunk in the range being deleted)
QTY	(the number of trunks being deleted, with criteria previously described)

All the other fields are populated with data of the first trunk to be deleted. and the string *Enter Delete, Validate, or Print:* is produced.

6. Enter **d** to complete the deletion.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen

Are any more trunks to be deleted?

- If **yes**, RETURN to step 4 or 5, whichever is appropriate, to delete additional trunks.
- If **no**, CONTINUE this procedure.

7. Enter **<** to return to the forms menu and **q** to exit RC/V.

8. Issue the input message:

OP:SS7,TG=a

on the MCC/STLWS, where **a** is the target TG, and check that the intended TG members were deleted (the string "NO DATA FOUND" is produced).

9. Back up the new ODD by entering the input message:

BKUP:ODD

on an MCC/STLWS.

10. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.2.5: Convert Existing Trunk Members

OVERVIEW

This procedure can be used to move multi-frequency (MF) trunks, or integrated services user part (ISUP) trunks currently controlled by a common network interface (CNI), to an ISUP trunk group (TG) terminated on a GSM's OPC. The term "move" actually represents the deletion of trunks from their original MF/CNI trunk group, followed by insertion of trunks into a GSM-controlled TG, reusing the same analog/digital facility access. Only MF trunks can be moved in 5ESS®-2000 switch VCDX offices, and movement of CNI trunks in a non-VCDX office requires installation of the 5E12 software release.

PROCEDURE

1. Is an **entire TG** to be converted to a GSM's control?

If so, EXIT this procedure immediately and execute the procedure, "Convert Existing Trunk Routes," Procedure 13.2.6.

2. Obtain a list of **MF/CNI trunks** to be moved. Issue the input message:

OP:LIST,TG=xx

on an MCC/STLWS, where **xx** is the target TG **from** which trunk members are to be extracted. Survey the office equipment listed for each of the target trunks, specifically the trunk equipment number (TEN), digital equipment number (DEN), or network equipment number (NEN). Note the **associated SM**, which is the **first argument** of the TEN, DEN, or NEN.

- If **any** of the identified office equipment resides on an SM that does **not** match the **target GSM**, EXIT this procedure. **All** trunks assigned to a TG with a GSM's OPC **must** reside on that GSM.
- If **all** of the identified office equipment resides on the GSM, record the TENs/DENs/NENs for reuse, and CONTINUE this procedure.

3. Has the **target TG** on the **GSM** to which trunk members are to be added already been provisioned?

- If the target TG has **not** been provisioned, execute the procedure "Add New ISUP Trunk Routes," Procedure 13.2.1, before continuing to the next step. The origination point code (OPC) used must correspond to the OPC provisioned for the target GSM.
- If the target TG **exists**, CONTINUE this procedure.

4. Use the procedure "Delete Trunk Members," Procedure 13.2.4, to **delete** the identified **MF/CNI** trunks, and then CONTINUE to the next step.

5. Use the procedure "Add New ISUP Trunk Members," Procedure 13.2.2, to **add** those trunks to the **target GSM TG**. Reuse the **office equipment** recorded in Step 2 as trunk access.

It should be noted that the new trunks should not be restored (new trunks exit RC transactions in an OOS-CADN-DSBLD state) until the far-end office completes conversion and testing is completed according to local practices.

6. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.2.6: Convert Existing Trunk Routes

OVERVIEW

This procedure can be used to move **entire** multi-frequency (MF) or integrated services user part (ISUP) trunk groups (TGs) currently controlled by a common network interface (CNI), to an ISUP TG terminated on a GSM's OPC. The term "move" actually represents the deletion of trunks from their original MF/CNI trunk group, followed by insertion of trunks into a GSM-controlled TG, reusing the same analog/digital facility access and route indexes, while minimizing the time when trunks are unavailable. Only MF TGs can be converted in 5ESS®-2000 switch VCDX offices. Conversion of CNI TGs in a non-VCDX office requires installation of the 5E12 software release.

This procedure allows reuse of existing route indexes associated with converted TGs.

PROCEDURE

1. Obtain a list of **MF/CNI trunks** to be moved from the **TG to be deleted**. Issue the input message:

OP:LIST,TG=xx

on an MCC/STLWS, where **xxx** is the **TG to be deleted**. Survey the office equipment listed for each trunk, specifically the trunk equipment number (TEN), digital equipment number (DEN), or network equipment number (NEN). Note the **associated SM**, which is the **first argument** of the TEN, DEN, or NEN.

- If **any** of the identified office equipment resides on an SM that does **not** match the **target GSM**, EXIT this procedure. **All** trunks assigned to a TG with a GSM's OPC **must** reside on that GSM.

Use the procedure "Delete Trunk Members," Procedure 13.2.4, to delete trunks **not** resident on the GSM, and reenter this procedure. Alternately, use the procedure "Convert Existing Trunk Members," Procedure 13.2.5, to move only selected trunks that **are** resident on the GSM.

- Otherwise, CONTINUE this procedure.

2. Issue the input message:

OP:OFR,FORM=5303,DEVICE=xxx

on an MCC/STLWS, to produce office records for the ROUTE INDEX (ROUTING) view. The device **xxx** is described in "Trunk Route Provisioning Overview," Procedure 13.2.

From the output produced, determine **all existing route indexes** that reference the **MF/ISUP TG to be deleted**. Decide whether these route indexes are to be assigned to the **new GSM TG**, or to be deleted entirely.

Will any of these route indexes be assigned to the new GSM TG?

- If **yes**, CONTINUE this procedure.
- Otherwise, SKIP to Step 5.

3. At an RC/V terminal, enter **10.2i** to access the ROUTE INDEX (ROUTING) view in INSERT mode. The intent of this step is to create a **temporary** (dummy) route index for the **MF/ISUP TG to be deleted**, to

allow manipulation of "real" route indexes identified in Step 2.

Enter the following data for the new route index:

RTI	(new, temporary route index)
ETYP	(route type)
TGN	(MF/ISUP TG to be deleted in this procedure)
NEXT RTI	(blank)

Enter other fields as defined in the 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)*, as determined by local practices. When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

4. Enter **i** to complete the insert.

When the insertion completes, "FORM INSERTED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu, and **q** to quit RC/V.

5. Has the **new TG** on the **GSM** already been provisioned?

— If that TG has **not** been provisioned, execute the procedure "Add New ISUP Trunk Routes," Procedure 13.2.1, before continuing to the next step. The origination point code (OPC) used **must** correspond to the OPC provisioned for the target GSM.

During the execution of that procedure, assign **new** route indexes only (if required), and do not consider any existing route indexes identified in Step 2.

— If the target GSM TG already **exists**, CONTINUE this procedure.

6. Are any of the route indexes identified in Step 2 to be **reassigned** to the **GSM TG**?

— If **yes**, CONTINUE this procedure.

— Otherwise, SKIP to Step 10.

7. At an RC/V terminal, enter **10.2u** to access the ROUTE INDEX (ROUTING) view in UPDATE mode.

Specify the key field:

RTI	(route index to be updated)

All other fields are populated with current values, and the string *Enter Update, Change, Validate, or Print:* is produced.

8. Enter **c** to start the change mode. The expected result is the *Change field:* string. Enter the **number of the field** to be updated to move the cursor to that field. Minimum changes required are:

TGN	(new GSM TG number)
NEXT RTI	(temporary RTI inserted in Step 3)

Any other changes in routing characteristics can be made according to local practices.

When all changes have been made, enter **<** to return to the command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu (if no updates to other route indexes are to be made) and q to quit RC/V (if no further route indexes are to be deleted).

9. Have all route indexes identified in Step 2 for reassignment to the GSM TG been updated?

— If **yes**, CONTINUE this procedure.

— If **no**, RETURN to Step 6.

10. Use the procedure "Delete Trunk Members," Procedure 13.2.4, to delete **some or all** members of the **MF/CNI TG to be deleted**.

Record the office equipment numbers (TENS, DENS, or NENS) of the deleted trunks, so they can be reused.

11. Use the procedure "Add New ISUP Trunk Members," Procedure 13.2.2, to insert the trunks referenced in Step 10 into the **new or existing GSM TG**.

Trunk characteristics may be different from the original trunks (per local practices), but the office equipment used for access (TENS, DENS, or NENS) should correspond to the list created in Step 10.

12. Have all the trunks in the original MF/CNI trunk group been moved?

— If **yes**, CONTINUE this procedure.

— If **no**, RETURN to Step 10.

13. Was a **temporary** (dummy) route index created in Step 3?

— If **yes**, CONTINUE this procedure.

— Otherwise, SKIP to Step 15.

14. The reference to the **temporary route index** associated with the **MF/CNI TG to be deleted** should be removed as an alternate route for route indexes assigned to the **GSM TG**.

At an RC/V terminal, enter **10.2u** to access the ROUTE INDEX (ROUTING) view in UPDATE mode.

Specify the key field:

RTI	(route index with temporary alternate route)

All other fields are populated with current values, and the string *Enter Update, Change, Validate, or Print:* is produced.

Enter **c** to start the change mode, and enter the number of the NEXT RTI field. Change the field to a valid alternate route, or enter ' (apostrophe) to blank the field (no alternate route). Then enter < to return to the command line and **u** to complete the update.

Repeat for other route indexes with the temporary alternate route. When all updates are complete, enter < to return to the forms menu.

15. Execute procedure "Delete Trunk Routes," Procedure 13.2.3, to delete the target **MF/CNI TG**, noting that the **temporary route index**, if defined in Step 3, will be deleted as an integral part of that procedure.

16. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3: SCCP PROVISIONING

OVERVIEW

The connectionless signaling connection control part (SCCP) capability provides the ability to route messages based on a global title (GT processing) within the GSM. SCCP routing and management within the GSM performs such GT processing, maintains status of destination routes, and uses the message transfer part (MTP) to transfer messages within the CCS network.

A GT is part of a called party address (contains the digit string of called number), which requires special processing by another office, such as a network control point (NCP) or a service control point (SCP), before the call can be completed. It also identifies the type of TCAP service provided.

A global title translation (GTT) involves translating a GT to a destination point code (DPC) and possibly a subsystem (a connectionless SCCP user in the destination DPC), where required services for the associated application are provided. If the GTT identifies both the DPC and subsystem destination, this is known as the *final GTT* (specifically, its final destination for GT processing); if only a destination DPC is identified (subsystem is designated as 0 in this case), this is known as an *intermediate GTT*, and that DPC has the knowledge to perform a GTT to forward the message toward the final destination.

The following additional terms will be encountered in the procedures that follow:

Translation type is the part of the global title that refers to a specific TCAP service (often an intelligent network service) that requires GTT treatment.

SCCP Translation Groups defines the 5ESS®-2000 switch implementation (a user-defined template) that describes how digits in a GT are to be translated locally. Two types of digit strings can be used to define a translation: a **fixed digit string** group requires one or more digits in the called party address to be present, in addition to variable primary and secondary digits, while a **non-fixed digit string** group allows variable primary and secondary digits.

SCCP Translation Tables associate a specific translation type to a specific translation group. A specific translation group may be referenced by more than one translation type. With the 5E12 software release, the translation type may be mapped directly to a DPC for remote GTT processing (described later).

SCCP Route Destinations are the recognized destinations to which a GT is sent for processing or forwarding to a final destination. This could be a DPC to support intermediate GTT processing or a DPC/SCCP subsystem for final GTT processing. Access to defined SCCP route destinations is monitored. A **primary** route is designated as a destination in a GTT; a **secondary** (or **backup**) route may be defined, which will be used only if access to the primary route is prohibited.

Local Global Title Translations refer to the detailed mapping of one or more digits in a called party address for a specific application (i.e., translation type) to an SCCP route destination, which will provide the required processing or further translations.

Remote Global Title Translations refer to cases where all GTs associated with an application (i.e., translation type) are sent to a remote DPC for GTT processing. It is assumed that the remote DPC has the knowledge to forward the message towards its final destination, and local analysis of digits is not required.

With the previous definitions in-hand, the following scenarios might be useful on first encounters with the extremely flexible global title translation capabilities available in a GSM environment.

- Before any GTTs or SCCP routes can be provisioned, the GSM must be prepared to provide SCCP functionality. This is accomplished by using the procedure "Grow Connectionless SCCP GSM," Section 13.3.1, and then adjusting any general timers/parameters associated with SCCP operation using the procedure

"Update SCCP Timers and Message Priorities," Section 13.3.2 .

- In some cases, the SCCP application (translation type) and the called party address is sufficient for the local office to determine the DPC and SSN of the remote data base or office to complete processing; this is called the "final GTT," as described previously. A more likely scenario involves an "intermediate GTT." In this case, global title messages originated on the switch contain only sufficient information to route the message to a remote signaling point chosen to perform further global title translations, which will forward the message to its final SCCP destination or another intermediate point code. Usually a local/regional signal transfer point (STP) pair represents these target intermediate signaling points. Ultimately, the final destination DPC/SSN will receive the message for processing, and a reply is sent back to the DPC/SSN of the originating switch associated with the calling party address.

Whether the final GTT destination (DPC and SSN) or an intermediate GTT (DPC and SSN 0, which implies the receiving switch must provide further analysis) is used, these SCCP route destinations must be explicitly known to the GSM. These can be provisioned using the procedure "Define Primary/Backup SCCP Route Destinations," Section 13.3.3 . The *primary* route specifies the destination where GTs will be sent (as provisioned) under normal circumstances; a *backup* destination can also be defined, which will be used only if the primary route is unavailable.

It should be noted that provisioned primary/backup routes mutually backup each other. For example, if DPC A is provisioned as a primary route, while DPC B is its backup, then data will also be created with DPC B as a primary route and DPC A is its backup. Thereafter, either DPC A or DPC B can be designated as an SCCP route destination. This arrangement is normally used for a mated STP pair performing intermediate GTTs.

An alternate to designating a mated pair of STPs as intermediate primary/backup route destinations is to define a *capability* (or *alias*) code for the pair. A capability code is a *single* point code that is recognized by both STPs in a mated pair as their point code for GTT processing; many STP pairs have such a code assigned to them. This special capability code can be defined as an ordinary DPC associated with a GSM, using the procedure "Define New Destination Point Codes," Section 13.1.7 , where normal access is a combined link set, whose members are link sets terminating on each STP in the mated pair. Such a DPC can then be defined as a primary SCCP route destination, with the net effect being SCCP traffic is load shared between the two STPs in the mated pair, noting no backup need be designated.

- If *local* global title translations are required, at least one translation group must be defined, along with the appropriate individual GTT to provide digit analysis. This is best illustrated by example.

For the first example, assume that a specific application requires that NPAs 312, 630, 773, and 847 be sent to a specific DPC/SSN for final GTT processing. In this case, a *non-fixed* digit translation group should be created with four individual GTTs, using the procedure "Define GTT Translation Groups with Non-Fixed Digit Strings," Section 13.3.4 . The group should define a primary digit string length of 3, with the number of translations in the group as 4. Individual GTTs should be defined in the same procedure, identifying each of the cited NPA codes as the *primary plus secondary digit string* and the same destination DPC/SSN identified for each GTT (recalling that the target DPC/SSN must be defined as a SCCP route destination).

For a second example, assume an "800 service" requires 800 numbers be sent to one STP pair for intermediate GTT analysis, while 888 numbers are to be analyzed by a second STP pair. In this case, a *fixed* digit translation group should be created with two individual GTTs, using the procedure "Define GTT Translation Groups with Fixed Digit Strings," Section 13.3.5 . The group should define a fixed digit string length of 1, a primary digit string length of 2; a subgroup with fixed digit 8 defined should be created with the maximum number of translations in the subgroup as 2. Individual GTTs should be defined in the same procedure, identifying a *fixed digit string* of 8 with 00 and 88 being the *primary plus secondary digit strings*, respectively, and the appropriate STP pair capability point code should be designated for each GTT (recalling that the target DPCs must be defined as SCCP route destinations).

The final step in either of the previous examples is to tie a particular TCAP application (identified by a

translation type) to the appropriate translation group just defined. Use procedure "Define SCCP Translation Table," Section 13.3.6 .

- If *remote* global title translations are required, "real" digit analysis need not be performed locally. In this case, a mated STP pair is usually specified as the destination for a specific application, regardless of the associated digit strings.

In the 5E11 software release, a translation group and GTTs must be defined. The most effective way to accomplish this task is to define a *non-fixed* digit translation group with ten individual GTTs, using the procedure "Define GTT Translation Groups with Non-Fixed Digit Strings," Section 13.3.4 . The group should define a primary digit string length of 1, with the number of translations in the group as 10. Individual GTTs should be defined in the same procedure, identifying a *primary plus secondary digit string* for each single digit in the range 0-9, and the same destination DPC corresponding to the capability code of the mated STP pair identified for each GTT (recalling that the target DPC must be defined as a SCCP route destination). If a capability code for the STP pair is not available, define each DPC in the pair as primary/backup SCCP route destination couplet, and have all *even* digit GTTs reference one STP and all *odd* digit GTTs reference the mate STP, to provide load sharing of the SCCP message traffic. The final step is to tie a particular TCAP application (identified by a translation type) to the translation group just defined, recalling that multiple translation types can be assigned to the *same translation group*, if desired.

In the 5E12 software release, remote GTT functionality can be defined directly without requiring the definition of any translation groups or GTTs. Use procedure "Define SCCP Translation Table," Section 13.3.6 , to directly associate a given translation type with a destination DPC. The target DPC must be defined as a SCCP route destination, and may be a capability code; if a capability code is not known, there is no way to load-share between a mated STP pair using this simplified approach.

- The final step is to allocate memory for SCCP data and activate SCCP functionality. This is accomplished by executing the pair of procedures "Begin SCCP Data Initialization," Section 13.3.7 , and "Activate Connectionless SCCP Processing," Section 13.3.8 . SCCP cannot be activated, unless at least one GTT is defined, or a remote GTT destination is defined (the latter case is only possible in the 5E12 software release).

See Table 13.3-1 for a list of RC/V views used to provision SCCP Components on a GSM.

Table 13.3-1 GSM SCCP RC/V Views

VIEW	TITLE	USE	PURPOSE
8.42	CCS TCAP APPLICATION	r	Verify TCAP application platform
16.20	SCCP NETWORKS DEFINITION	id	Allocate memory for SCCP translation data
16.21	SCCP PARAMETER DEFINITION	u	Update SCCP timers and message priorities
16.22	SCCP PRIMARY/BACKUP DESTINATION	iudr	Define primary/backup SCCP route destinations
16.23	SCCP TRANSLATION GROUP MASK	iud	Define SCCP translation group
16.24	SCCP TRANSLATION TABLE	iud	Define SCCP translation table
16.25	SCCP SINGLE GLOBAL TITLE TRANSLATION	iud	Define individual global title translations
Note: The USE column indicates how the view is used: r for REVIEW, i for insert, u for UPDATE, and d for DELETE.			

Tables 13.3-2 , 13.3-3 , and 13.3-4 contain lists of procedures to grow, update and delete connectionless SCCP. Each list shows the sequence of procedures to use for each activity. The remainder of this section contains each procedure listed in the tables.

Each procedure provides a series of actions that must be completed in the sequence given. Any deviation from the sequence jeopardizes the process and may affect customer calls. During the procedures, do not use input messages, other than those identified in the document.

The procedures listed in Table 13.3-2 are used to provision and activate SCCP functionality in a GSM. Recall that Sequence number 4A/4B are optional in the 5E12 software release, if only *remote GTT* processing is required. Also in the 5E12 software release, a TCAP application must be specifically assigned to use the GSM signaling platform before the SCCP GSM will be used for GTT or SCCP transport. See "TCAP Application Platform Provisioning," Section 13.5, for more details.

Table 13.3-2 SCCP Growth Procedures

SEQUENCE	JOB DESCRIPTION	PROCEDURE
1	Grow connectionless SCCP GSM	Procedure 13.3.1
2	Update SCCP Timers and Message Priorities	Procedure 13.3.2
3	Define Primary/Backup SCCP Route Destinations	Procedure 13.3.3
4A	Define GTT Translation Groups with Non-Fixed Digit Strings	Procedure 13.3.4
4B	Define GTT Translation Groups with Fixed Digit Strings	Procedure 13.3.5
5	Define SCCP Translation Table	Procedure 13.3.6
6	Begin SCCP Data Initialization	Procedure 13.3.7
7	Activate connectionless SCCP Processing	Procedure 13.3.8

Before initiating the procedures, verify the GSM being equipped has the minimum of 2-Mb (megabyte) spare memory to be allocated for the feature.

To update SCCP provisioning, use the procedures listed in Table 13.3-3.

Table 13.3-3 SCCP Updating Procedures

SEQUENCE	JOB DESCRIPTION	PROCEDURE
1	Update SCCP Timers and Message Priorities	Procedure 13.3.2
2	Update Backup SCCP Route Destinations	Procedure 13.3.9
3	Update SCCP Translation Group	Procedure 13.3.10
4A	Define Single GTT with Non-Fixed Digit String	Procedure 13.3.11
4B	Define Single GTT with Fixed Digit String	Procedure 13.3.12
5A	Update Single GTT with Non-Fixed Digit String	Procedure 13.3.13
5B	Update Single GTT with Fixed Digit String	Procedure 13.3.14
6	Update SCCP Translation Table	Procedure 13.3.15

To delete SCCP provisioning use the procedures in the sequence listed in Table 13.3-4. At the completion of these procedures, SCCP will be completely degrown and deactivated.

Table 13.3-4 SCCP Deletion Procedures

SEQUENCE	JOB DESCRIPTION	PROCEDURE
1A	Delete Single GTT with Non-Fixed Digit String	Procedure 13.3.16
1B	Delete Single GTT with Fixed Digit String	Procedure 13.3.17
2	Delete SCCP Translation Table	Procedure 13.3.18
3	Delete SCCP Translation Group	Procedure 13.3.19
4	Delete Primary SCCP Route Destinations	Procedure 13.3.20
5	Deactivate Connectionless SCCP Processing	Procedure 13.3.21
6	Delete SCCP GSM	Procedure 13.3.22

Some of the procedures that follow require specific **office records** be interrogated. In those procedures, an input command of the form

OP:OFR, FORM=###, DEVICE=xxx

will be specified. If **xxx** is "FILE", the office records will be deposited in a file /rclog/OFR.Oy, where **y** is the **REQUEST ID** in the command response; the file can be interrogated or printed according to local procedures. Alternately, if **xxx** is specified as "ttyR", output is produced directly on the resident office records printer (if available); other output destinations are possible, as defined on the **OP-OFR** input manual page in 235-600-700, *Input Messages Manual*.

For detailed descriptions of all recent change views (RC/V) see 235-118-2xx, *Recent Change Reference* or

235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)*. For protocol information refer to the *ANSI®* standard T1.112-1992, *Signaling System Number 7 (SS7) Signaling Connection Control Part (SCCP)*.

The SCCP provisioning procedures in this section are:

PROCEDURE

1. Procedure 13.3.1 - Grow Connectionless SCCP GSM
2. Procedure 13.3.2 - Update SCCP Timers and Message Priorities
3. Procedure 13.3.3 - Define Primary/Backup SCCP Route Destinations
4. Procedure 13.3.4 - Define GTT Translation Groups with Non-Fixed Digit Strings
5. Procedure 13.3.5 - Define GTT Translation Groups with Fixed Digit Strings
6. Procedure 13.3.6 - Define SCCP Translation Table
7. Procedure 13.3.7 - Begin SCCP Data Initialization
8. Procedure 13.3.8 - Activate Connectionless SCCP Processing
9. Procedure 13.3.9 - Update Backup SCCP Route Destinations
10. Procedure 13.3.10 - Update SCCP Translation Group
11. Procedure 13.3.11 - Define Single GTT with Non-Fixed Digit Strings
12. Procedure 13.3.12 - Define Single GTT with Fixed Digit Strings
13. Procedure 13.3.13 - Update Single GTT with Non-Fixed Digit Strings
14. Procedure 13.3.14 - Update Single GTT with Fixed Digit Strings
15. Procedure 13.3.15 - Update SCCP Translation Table
16. Procedure 13.3.16 - Delete Single GTT with Non-Fixed Digit Strings
17. Procedure 13.3.17 - Delete Single GTT with Fixed Digit Strings
18. Procedure 13.3.18 - Delete SCCP Translation Table
19. Procedure 13.3.19 - Delete SCCP Translation Group
20. Procedure 13.3.20 - Delete Primary SCCP Route Destinations
21. Procedure 13.3.21 - Deactivate Connectionless SCCP Processing
22. Procedure 13.3.22 - Delete Connectionless SCCP GSM

Procedure 13.3.1: Grow Connectionless SCCP GSM

OVERVIEW

The connectionless signaling connection control part (SCCP) global switching module (GSM) is grown first using this procedure to allocate memory for translation data. The target SM must be provisioned as a GSM, or this procedure will fail.

PROCEDURE

1. Determine if the target SM/SM-2000 is defined as a GSM by issuing the input message:

OP : CCS , GSM , SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM number.

- If the request fails (response "NG - GSM MISMATCH" or "NG - NO GLOBAL SM IN OFFICE"), the target SM/SM-2000 has not yet been defined as a GSM; EXIT this procedure immediately.

Use the procedure "Convert to a CCS Global Switching Module," Section 13.1.1, to provision the GSM, and then RESTART this procedure.

- If the request succeeds, the GSM has already been defined, and this procedure is appropriate; CONTINUE this procedure.

2. At an RC/V terminal, enter **16.20i** to access the SCCP NETWORKS DEFINITION view in INSERT mode.

Enter the following data:

GSM	(target GSM number)

When the GSM is entered, the string *Enter Insert, Validate, or Print:* is produced.

3. Enter **i** to complete the insertion.

- If the insertion completes successfully, "FORM INSERTED" flashes in the upper right corner of the screen. Enter **<** to return to the forms menu and **q** to quit recent change.

Before continuing, monitor the ROP for messages indicating the success of the allocation of an optional data region (ODR) for the GSM's pumpable SCCP translation tables (target image SCCP); be patient, as response is highly dependent on SM occupancy. After the output messages

```
CFR SPRMEM IMAGE=SCCP SM=xxx TYPE=GROW COMPLETED
CFR SPRMEM IMAGE=SPAREMEM SM=xxx TYPE=GROW COMPLETED
MEMORY POINTERS UPDATED - ODD BACKUP REQUIRED
```

appear in the 5E11 software release (where **xxx** is the target GSM), the allocation of the SCCP image was successful. This process may have "stolen" stand-alone billing memory (SABM) to accomplish the allocation. The current size of SABM should be verified and possibly be grown according to local practices; refer to *5ESS®-2000 Switch Engineering Information, Index 8* for guidance.

In the 5E12 software release, a slightly different output will appear, specifically:

```
CFR SPRMEM ODRID=SCCP SM=xxx TYPE=GROW COMPLETED
CFR SPRMEM ODRID=SPAREMEM SM=xxx TYPE=GROW COMPLETED
MEMORY POINTERS UPDATED - ODD BACKUP REQUIRED
```

As allocation of ODRs in 5E12 use *only SPARE MEMORY*, the size of the SABM region has *not* changed.

SKIP to Step 5.

- If the target GSM is already provisioned for SCCP functionality, "DUPLICATE FORM" flashes in the upper right corner of the screen. Enter < to return to the forms menu and **q** to quit recent change.

EXIT this procedure immediately, as it is inappropriate.

- Otherwise, the attempted provisioning has failed. Enter < to return to the forms menu and **q** to quit recent change, and CONTINUE this procedure.

4. Monitor the ROP for messages indicating the failure of the allocation of an ODR for the SCCP image. Follow the instructions, based upon the nature of the message produced:

- The following output message

```
CFR SPRMEM IMAGE=SCCP SM=xxx TYPE=GROW FAILED
SABM SHRINKAGE FAILURE
```

could appear in the 5E11 software release, where **xxx** is the target GSM.

This message indicates an attempt to shrink SABM to provide enough spare memory for ODR allocation has failed, as the SABM region contains active records. Exit this procedure now, and reenter later after billing records have been offloaded.

- The following output message

```
CFR SPRMEM IMAGE=SCCP SM=xxx TYPE=GROW FAILED
INSUFFICIENT SPARE SM MEMORY
```

could appear in the 5E11 software release, where **xxx** is the target GSM.

In this case, ODR growth cannot be accomplished (even if SABM in excess of the required minimum is converted to spare memory) and new physical memory must be grown. Use *PROCEDURE 3.27, Perform SM Memory Growth Procedure* in the 235-105-231, 5ESS®-2000 Switch Hardware Change Procedures - Growth document, and then reenter this procedure.

- The following output message

```
CFR SPRMEM ODRID=SCCP SM=xxx TYPE=GROW FAILED
INSUFFICIENT SPARE SM MEMORY
```

could appear in the 5E12 software release, where **xxx** is the target GSM.

In this software release, a failure in the allocation of an ODR for a target SCCP image indicates only that sufficient SPARE MEMORY is not available, but engineerable memory regions for SABM or real-time billing memory (RTBM) can be reduced according to local practices, rather than growing in new physical memory.

In addition to the above failure indication, additional data will indicate the size of the desired SCCP image, the size of current spare memory, the sizes of current SABM and RTBM regions (if provisioned), as well as the amount of SABM/RTBM memory that can be reconfigured into spare memory which can be used for ODR allocation. If the sum of spare memory, plus the configurable segment of SABM/RTBM memory is sufficient to allocate the SCCP image, appropriate SABM/RTBM degrowth can be considered. If according to local practices, sufficient degrowth of SABM/RTBM regions can be accomplished, this procedure should be reentered. See *5ESS®-2000 Switch Engineering Information, Index 8* for guidance in degrowing the SABM region, and 235-200-110, *5ESS®-2000 Switch Long Distance Platform Document* for guidance in degrowing the RTBM region.

If sufficient degrowth of SABM/RTBM regions is not possible, new physical memory must be grown. Use *PROCEDURE 3.27, Perform SM Memory Growth Procedure* in the 235-105-231, *5ESS®-2000 Switch Hardware Change Procedures - Growth* document, and then reenter this procedure.

5. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

6. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.2: Update SCCP Timers and Message Priorities

OVERVIEW

This procedure is used to change default SCCP parameters during initial provisioning of the feature on a GSM, or to update those parameters at any time on an existing SCCP GSM.

Before beginning this procedure, all SCCP timer values and message priorities should be predetermined, consulting 235-080-100, *5ESS®-2000 Switch Translation Guide (TG5)*.

PROCEDURE

1. At an RC/V terminal, enter **16.21u** to access the SCCP PARAMETERS DEFINITION view in UPDATE mode.

Specify the key field:

GSM	(target GSM number)

- If "FORM NOT FOUND" flashes in the upper right corner of the screen, the target GSM is not provisioned for SCCP use. EXIT this procedure immediately and use the procedure "Grow Connectionless SCCP GSM," Section 13.3.1, to define an SCCP GSM.
- Otherwise, all other fields on the view are populated with current values and the string *Enter Update, Change, Validate, or Print:* is produced. CONTINUE this procedure.

2. Enter **c** to start the change mode. The expected response is the *Change field:* string.

Enter the field number and data for each field that requires changing.

NOTE: Do not change the value of the INIT STATUS or PROCESSING fields as part of this procedure.

3. Enter **<** to exit changes mode and **u** to update the data.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

4. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

5. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.3: Define Primary/Backup SCCP Route Destinations

OVERVIEW

This procedure defines the primary and optional backup SCCP route destination, which is the destination point code (DPC) and the subsystem number, used for the global title translation (GTT) and network management on a specific global switching module (GSM).

Before entering this procedure, administrators should be aware of the following constraints:

- The DPCs specified as primary or backup destinations must be defined for the target GSM, which must be a provisioned "SCCP GSM."
- It is possible to provision multiple primary or primary/backup routes, but a given DPC/subsystem combination can be assigned *only one* primary or backup route destination. Primary and backup routes must be provisioned on the *same* SCCP GSM.
- If a backup route is defined, the primary/backup routes provide *mutual alternate SCCP destinations*. Therefore, if destination *A* is defined as a primary route, and destination *B* is its backup route by this procedure, then ODD is also generated for destination *B* as a *primary* route, with destination *A* as its *backup*. This can be verified by invoking RC/V view 16.22 in review mode.

PROCEDURE

1. At an RC/V terminal, enter **16.22i** to access the SCCP PRIMARY/BACKUP DESTINATION view in INSERT mode.

Enter the following data:

GSM PRIMARY	(target GSM number)
DPC PRIMARY	(9-digit primary DPC)
SSN PRIMARY	(primary subsystem number)

The subsystem number (SSN PRIMARY field) is 0 if no subsystem is identified, or 2-225 for a unique reference.

2. Populate appropriate backup DPC information (if a backup route is desired):

GSM BACKUP	(target GSM number)
DPC BACKUP	(9-digit backup DPC)
SSN BACKUP	(backup subsystem number)

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

3. Enter **i** to complete the insert.
 - If "FORM INSERTED" flashes in the upper right corner of the screen, the insertion has completed successfully. Enter **<** to return to the forms menu, **q** to exit RC/V, and then CONTINUE this procedure.
 - If the insert fails due to the fact that the target GSM is not provisioned for SCCP use, EXIT this procedure immediately. Use the procedure "Grow Connectionless SCCP GSM," Section 13.3.1, to define an SCCP GSM, and then reenter this procedure.
 - If the insert fails due to the fact that the designated primary or backup DPC is not provisioned, EXIT this

procedure immediately. Use the procedure "Define New Destination Point Codes," Section 13.1.7 , to define the missing DPC, or choose another SCCP route destination before reentering this procedure.

4. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

5. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.4: Define GTT Translation Groups with Non-Fixed Digit Strings

OVERVIEW

This procedure assigns a new SCCP translation group using **non-fixed** (primary plus secondary) digit strings, as well as the group's associated global title translation (GTT) data.

Due to the potential complexity of the data entered, it is imperative that administrators have accurate translation data prepared in advance according to local practices, consulting 235-080-100, *5ESS®-2000 Switch Translation Guide (TG5)*.

Finally, any DPC/subsystem designated in a GTT must be provisioned as a primary or backup route destination on the target SCCP GSM.

PROCEDURE

1. At an RC/V terminal, enter **16.23i** to access the SCCP TRANSLATION GROUP MASK view in INSERT mode.

Enter the following data:

GSM	(target SCCP GSM number)
TRANS GROUP	(new translation group in range 0-63)
NUM FIXED DIGITS	(enter 0)
NUM PRIM DIGITS	(number of primary digits in range 1-10)
NUM SEC DIGITS	(number of secondary digits in range 0-9)
STRING MATCH	(type of match: FULL, PART, VAR)
PRIM PLUS SEC	(maximum number of translations in group)

Note that the **total number** of primary **plus** secondary digits specified cannot exceed 10. Also, the maximum number of translations associated with **all** SCCP translation groups combined is 131071.

2. Enter **i** to complete the insert.
 - If "FORM INSERTED" flashes in the upper right corner of the screen, the insertion has successfully completed. Enter **<** to return to the forms menu, and CONTINUE this procedure.
 - If the insert fails due to the fact that the target GSM is not provisioned for SCCP use, EXIT this procedure immediately. Use the procedure "Grow Connectionless SCCP GSM," Section 13.3.1, to define an SCCP GSM, and then reenter this procedure.
 - If the insert fails due to the fact that the target translation group already exists, EXIT this procedure immediately. Either choose a new translation group, or use the procedure "Define Single GTT with Non-Fixed Digit String," Section 13.3.11, to add new GTTs to an existing group.
3. At the RC/V terminal, enter **16.25i** to access the SCCP SINGLE GLOBAL TITLE TRANSLATION view in INSERT mode.

Enter the following data for one of the primary/secondary digit strings associated with the new translation group.

GSM	(target SCCP GSM number)
TRANS GROUP	(parent translation group number)
FIX DIG STR	(leave this field blank)
PRIM PLUS SEC DIG STR	(see below)

MAX TRANS	(leave this field blank)
DEST GSM	(target SCCP GSM number)
DPC	(9-digit primary/backup DPC)
DEST SS NUM	(primary/backup destination subsystem number)

The number of digits entered in the PRIM PLUS SEC DIG STR field should be less than or equal to the total count specified for the parent translation group in Step 1; each digit can be in the range 0-9. The subsystem number (DEST SS NUM field) is 0 if no subsystem is identified, or 2-225 for a unique reference.

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

4. Enter **i** to insert the data.

- If "FORM INSERTED" flashes in the upper right corner of the screen, the insertion has successfully completed. CONTINUE this procedure.
- If the insert fails due to the fact that the target DPC/destination subsystem number is not a valid SCCP route destination for the target GSM, EXIT this procedure immediately. Use the procedure "Define Primary/Backup SCCP Route Destinations," Section 13.3.3, to define the missing routes before reentering this procedure.

5. Are there more primary/secondary digit strings to be defined?

- If **yes**, RETURN to Step 3.
- If **no**, CONTINUE this procedure.

6. Enter **<** to return to the forms menu and **q** to exit RC/V.

7. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

8. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.5: Define GTT Translation Groups with Fixed Digit Strings

OVERVIEW

This procedure assigns a new SCCP translation group using **fixed** digit strings, as well as the group's associated global title translation (GTT) data.

Due to the potential complexity of the data entered, it is imperative that administrators have accurate translation data prepared in advance according to local practices, consulting 235-080-100, *5ESS®-2000 Switch Translation Guide (TG5)*.

Finally, any DPC/subsystem designated in a GTT must be provisioned as a primary or backup route destination on the target SCCP GSM.

PROCEDURE

1. At an RC/V terminal, enter **16.23i** to access the SCCP TRANSLATION GROUP MASK view in INSERT mode.

Enter the following data:

GSM	(target SCCP GSM number)
TRANS GROUP	(new translation group in range 0-63)
NUM FIXED DIGITS	(number of fixed digits in range 1-6)
NUM PRIM DIGITS	(number of primary digits in range 1-10)
NUM SEC DIGITS	(number of secondary digits in range 0-9)
STRING MATCH	(type of match: FULL, PART, VAR)
PRIM PWS SEC	(leave this field blank)

Note that the **total number** of fixed **plus** primary **plus** secondary digits specified cannot exceed 12.

2. Enter **i** to complete the insert.
 - If "FORM INSERTED" flashes in the upper right corner of the screen, the insertion has successfully completed. Enter **<** to return to the forms menu, and CONTINUE this procedure.
 - If the insert fails due to the fact that the target GSM is not provisioned for SCCP use, EXIT this procedure immediately. Use the procedure "Grow Connectionless SCCP GSM," Section 13.3.1, to define an SCCP GSM, and then reenter this procedure.
 - If the insert fails due to the fact that the target translation group already exists, EXIT this procedure immediately. Either choose a new translation group, or use the procedure "Define Single GTT with Fixed Digit String," Section 13.3.12, to add new GTTs to an existing group.
3. At an RC/V terminal, enter **16.25i** to access the SCCP SINGLE GLOBAL TITLE TRANSLATION view in INSERT mode.

Enter the following data to establish a translation subgroup associated with a particular fixed string:

GSM	(target SCCP GSM number)
TRANS GROUP	(parent translation group)
FIX DIG STR	(see below)
PRIM PLUS SEC DIG STR	(leave this field blank)
MAX TRANS	(maximum number of translations for this fixed digit string)
DEST GSM	(blank)
DPC	(blank)

DEST SS NUM	(blank)

The **number** of fixed string digits (FIX DIG STR field) entered must correspond to the number (NUM FIXED DIGITS field) specified for the parent translation group in Step 1; each digit can be in the range 0-9. Also, the maximum number of translations associated with **all** SCCP translation groups combined is 131071.

4. Enter **i** to complete the insert.

When the insertion completes, "FORM INSERTED" flashes in the upper right corner of the screen.

5. Are there more fixed digit strings to be defined for this translation group?

- If **yes**, RETURN to Step 3.
- If **no**, CONTINUE this procedure.

6. Enter the following data for one of the primary/secondary digit strings associated with a particular fixed digit string subgroup.

GSM	(target SCCP GSM number)
TRANS GROUP	(parent translation group)
FIX DIG STR	(target fixed digit string)
PRIM PLUS SEC DIG STR	(see below)
MAX TRANS	(leave this field blank)
DEST GSM	(target SCCP GSM number)
DPC	(9-digit primary/backup DPC)
DEST SS NUM	(primary/backup destination subsystem number)

The number of digits entered in the PRIM PLUS SEC DIG STR field should be less than or equal to the total count specified for the parent translation group (sum of NUM PRIM DIGITS plus NUM SEC DIGITS) in Step 1; each digit can be in the range 0-9. The subsystem number (DEST SS NUM field) is 0 if no subsystem is identified, or 2-225 for a unique reference.

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

7. Enter **i** to insert the data.

- If "FORM INSERTED" flashes in the upper right corner of the screen, the insertion has successfully completed. CONTINUE this procedure.
- If the insert fails due to the fact that the target DPC/destination subsystem number is not a valid SCCP route destination for the target GSM, EXIT this procedure immediately. Use the procedure "Define Primary/Backup SCCP Route Destinations," Section 13.3.3, to define the missing routes before reentering this procedure.

8. Are there more primary/secondary digit strings to be defined for this translation group?

- If **yes**, RETURN to Step 6.
- If **no**, CONTINUE this procedure.

9. Enter **<** to return to the forms menu and **q** to exit RC/V.

10. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

11. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.6: Define SCCP Translation Table

OVERVIEW

During global title translation (GTT), the called party address will receive GTT treatment. Use this procedure to correlate a TCAP application (translation type) to a specific translation group; multiple translation types can be associated with the same translation group. The specified translation group must be defined for the target SCCP GSM.

With the 5E12 software release, it is possible to directly correlate a given translation type to a DPC for *remote GTT processing*. In this case, no translation group is referenced, but the remote DPC specified must be known as an SCCP route destination on the GSM.

PROCEDURE

1. Is **remote GTT processing** desired for the target translation type, **and** the switch is operating on the **5E12** software release?
 - If **yes**, SKIP to Step 4.
 - If **no**, CONTINUE this procedure to provision local GTT processing.
2. At an RC/V terminal, enter **16.24i** to access the SCCP TRANSLATION TABLE view in INSERT mode.

Enter the following data:

GSM	(target SCCP GSM number)
TRANS TYPE	(target translation type in range 0-255)
TRANS GROUP	(target translation group in range 0-63)
START GTT DIGIT	(digit to begin analysis)

In the 5E12 software release, the field **DPC** will also be present, and it should be left **blank**. When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

3. Enter **i** to complete the insert.
 - If "FORM INSERTED" flashes in the upper right corner of the screen, the insertion has completed successfully. Enter **<** to return to the forms menu and **q** to quit RC/V, and SKIP to Step 6.
 - If the insertion fails due to the fact that the target translation group is not defined on the GSM, EXIT this procedure immediately. Use the procedure "Define GTT Translation Groups with Non-Fixed Digit Strings," Section 13.3.4, or "Define GTT Translation Groups with Fixed Digit Strings," Section 13.3.5, to define the missing translation group, and then restart this procedure.
4. At an RC/V terminal, enter **16.24i** to access the SCCP TRANSLATION TABLE view in INSERT mode, recalling the 5E12 software release is required to provision *remote GTT processing*.

Enter the following data:

GSM	(target SCCP GSM number)
TRANS TYPE	(target translation type in the range 0-255)
TRANS GROUP	(leave blank)
START GTT DIGIT	(leave blank)
DPC	(target DPC providing remote GTT processing)

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

5. Enter i to complete the insert.
 - If "FORM INSERTED" flashes in the upper right corner of the screen, the insertion has successfully completed. Enter < to return to the forms menu, and CONTINUE this procedure.
 - If the insert fails due to the fact that the target GSM is not provisioned for SCCP use, EXIT this procedure immediately. Use the procedure "Grow Connectionless SCCP GSM," Section 13.3.1 , to define an SCCP GSM, and then reenter this procedure.
 - If the insert fails due to the fact that the target DPC is not a valid SCCP route destination for the target GSM, EXIT this procedure immediately. Use the procedure "Define Primary/Backup SCCP Route Destinations," Section 13.3.3 , to define the missing routes before reentering this procedure.
6. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.
7. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.7: Begin SCCP Data Initialization

OVERVIEW

If this is the initial growth of an SCCP GSM, two procedures are necessary to activate the connectionless SCCP. It is assumed that all SCCP routes and translation data have been defined, and all ODD backups are complete.

This procedure begins the data initialization for the connectionless SCCP on a specific GSM, by placing the SCCP in the operational state. After the NORMAL state is observed on the 1010 MCC page for the target GSM, connectionless SCCP processing is activated using the next procedure "Activate Connectionless SCCP Processing," Procedure 13.3.8.

PROCEDURE

1. At an RC/V terminal, enter **16.21u** to access the SCCP PARAMETER DEFINITION view in UPDATE mode.

Specify the key field:

GSM (target SCCP GSM number)

All the other fields are populated with current values and the string *Enter Update, Change, Validate, or Print:* is produced.

2. Enter **c** to start the change mode. The expected response is the *Change field:* string.

Enter the number for the INIT STATUS field and enter the following data:

INIT STATUS	OPER

3. Enter **u** to update the data.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu.

4. At the ROP, observe the following message:

```
INIT SCCP SM=x STARTED
LEVEL=SCCPINIT
```

where **x** is the target GSM number.

5. After a delay (the SCCP initialization process can take from one minute to an hour), what is the final status observed on the ROP report?

— If the final status is shown as

```
INIT SCCP SM=x COMPLETED
LEVEL=SCCPINIT
```

CONTINUE with the procedure in "Activate Connectionless SCCP Processing," Procedure 13.3.8.

— If, however, the initialization is unsuccessful, the following message will be produced:

```
INIT SCCP SM=x FAILURE EVENT=0
```

-## ##### ##

where ## ##### is the failure code. In this case, STOP this procedure immediately and contact technical support personnel according to local practices.

6. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.8: Activate Connectionless SCCP Processing

OVERVIEW

The final step in growing a new SCCP GSM is to activate the SCCP processing using this procedure.

Before activating SCCP processing, it is required that at least one global title translation (GTT) be defined in the 5E11 software release; in the 5E12 software release, either one GTT must be defined or at least one remote GTT DPC must be provisioned.

PROCEDURE

1. At an RC/V terminal, enter **16.21u** to access the SCCP PARAMETER DEFINITION view in UPDATE mode.

Specify the key field:

GSM	(target GSM number)

All the other fields are populated with current values and the string *Enter Update, Change, Validate, or Print:* is produced.

2. Enter **c** to start the change mode. The expected response is the *Change field:* string.

Enter the number for the PROCESSING field and enter **Y** (for YES).

3. Enter **u** to update the data.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

4. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

5. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.9: Update Backup SCCP Route Destinations

OVERVIEW

This procedure updates (or deletes) a **backup** SCCP route destination.

There is no way to update a **primary** SCCP route destination. Such primary routes must first be deleted (using "Delete Primary SCCP Route Destinations," Procedure 13.3.20), followed by the definition of a new primary route (using "Define Primary/Backup SCCP Route Destinations," Procedure 13.3.3).

It should be noted that GTTs which reference the **original** backup SCCP route do **not** have to be deleted, as that SCCP route is also defined in the ODD as a **primary route** (which is not altered by this procedure). Dependent upon the intent of this procedure, it may be necessary to update GTT route destinations to reference the new backup route (using "Update Single GTT with Non-Fixed Digit Strings," Procedure 13.3.13 , or "Update Single GTT with Fixed Digit Strings," Procedure 13.3.14), and/or delete the primary SCCP route that is equivalent to the original backup route (see "Delete Primary SCCP Route Destinations," Procedure 13.3.20).

New backup DPC destinations must be defined for the target GSM.

PROCEDURE

1. At an RC/V terminal, enter **16.22u** to access the SCCP PRIMARY/BACKUP DESTINATION view in UPDATE mode.

Enter the following key data:

GSM PRIMARY	(target SCCP GSM number)
DPC PRIMARY	(9-digit primary DPC)
SSN PRIMARY	(primary subsystem number)

These fields are displayed with current values:

GSM BACKUP	(target SCCP GSM number)
DPC BACKUP	(original backup DPC)
SSN BACKUP	(original backup subsystem number)

and the string *Enter Update, Change, Validate, or Print:* is produced.

2. Is the backup route destination to be updated or deleted by this procedure?
 - If the backup route destination is to be **deleted**, CONTINUE this procedure.
 - If the backup route destination is to be **updated**, SKIP to Step 4.

3. Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the GSM BACKUP field and **blank** that field (enter ' or apostrophe). Repeat for the DPC BACKUP and SSN BACKUP fields. Then skip to Step 5.

Recall that the deleted backup route destination still exists as a primary route destination (as previously noted), but the binding between the original SCCP routes in this view (as determined in Step 1) is broken.

4. Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the DPC BACKUP or SSN BACKUP field, and enter the new value; the GSM BACKUP

field cannot be updated. Repeat for the second field, if required. Then CONTINUE this procedure.

For **primary route A**, **original backup route B** and **updated backup route C**, the following relations will exist in the ODD. As previously noted, primary route B still exists, but route A is no longer its backup. Also, new reciprocal relations are created: primary route A with backup route C, and primary route C with backup route A.

5. When all data is entered, the string *Enter Update, Change, Validate, or Print:* is produced.

Enter **u** to update the data.

- If "FORM UPDATED" flashes in the upper right corner of the screen, the update has successfully completed. Enter < to return to the forms menu and **q** to exit RC/V, and CONTINUE this procedure.
- If the update fails due to the fact that the designated backup DPC is not provisioned, EXIT this procedure immediately. Use the procedure "Define New Destination Point Codes," Section 13.1.7, to define the missing DPC, or choose another SCCP route destination before reentering this procedure.

6. Back up the ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

7. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.10: Update SCCP Translation Group

OVERVIEW

This procedure updates the characteristics of a specific existing SCCP translation group.

PROCEDURE

1. At an RC/V terminal, enter **16.23u** to access the SCCP TRANSLATION GROUP MASK view in UPDATE mode.

Enter the following key data:

GSM	(target SCCP GSM number)
TRANS GROUP	(target translation group)

The following fields will appear, populated with current data:

NUM FIXED DIGITS	(number of fixed digits in fixed digit group)
NUM PRIM DIGITS	(number of primary digits)
NUM SEC DIGITS	(number of secondary digits)
STRING MATCH	(type of string match)
PRIM PLUS SEC	(maximum translations in non-fixed digit group)

and the string *Enter Update, Change, Validate, or Print:* is produced.

2. Enter **c** to start the change mode. The expected response is the *Change field:* string.

NOTE 1: Before changing the NUM FIXED, NUM PRIM or NUM SEC fields, all translations assigned to this translations group must be deleted using the procedure "Delete Single GTT with Non-Fixed Digit String," Procedure 13.3.16, or "Delete Single GTT with Fixed Digit String," Procedure 13.3.17, as appropriate.

NOTE 2: Before changing the PRIM PLUS SEC field, all translations assigned to this translation group must be deleted using the procedure "Delete Single GTT with Non-Fixed Digit String," Procedure 13.3.16, or "Delete Single GTT with Fixed Digit String," Procedure 13.3.17, as appropriate. Alternatively, SCCP can be deactivated using the procedure "Deactivate Connectionless SCCP Processing," 13.3.21.

Enter the field number to move to that field, and then enter the desired data. After the data is entered the *Change field:* prompt will reappear; repeat this procedure until all desired changes are made.

When all changes are completed, enter **return** to access the main menu; the string *Enter Update, Change, Validate, or Print:* is produced.

3. Enter **u** to update the data.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

4. If individual GTTs have been deleted according to either note in Step 2 to accomplish the update of an SCCP translation group, they should now be reinserted. Use the procedure, "Define Single GTT with Non-Fixed Digit String," Procedure 13.3.11, or "Define Single GTT with Fixed Digit String," Procedure 13.3.12, as appropriate.

If SCCP processing was deactivated, reactivate it using the procedure "Begin SCCP Data Initialization," Section 13.3.7 .

5. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

6. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.11: Define Single GTT with Non-Fixed Digit String

OVERVIEW

This procedure defines an individual global title translation (GTT) using a **non-fixed** digit string, when the parent SCCP translation group is already defined.

The maximum number of translations allocated for the parent SCCP translation group must be large enough to accommodate existing GTTs **plus** any new GTTs defined by this procedure. Otherwise, this procedure will fail.

Due to the potential complexity of the data entered, it is imperative that administrators have accurate translation data prepared in advance according to local practices, consulting 235-080-100, *5ESS®-2000 Switch Translation Guide (TG5)*.

Finally, any DPC/subsystem designated in a GTT must be provisioned as a primary or backup route destination on the target SCCP GSM.

PROCEDURE

1. At an RC/V terminal, enter **16.25i** to access the SCCP SINGLE GLOBAL TITLE TRANSLATION view in INSERT mode.

Enter the following data for each primary/secondary digit string.

GSM	(target SCCP GSM number)
TRANS GROUP	(parent translation group number)
FIX DIG STR	(leave this field blank)
PRIM PLUS SEC DIG STR	(see below)
MAX TRANS	(leave this field blank)
DEST GSM	(target SCCP GSM number)
DPC	(9-digit primary/backup DPC)
DEST SS NUM	(primary/backup destination subsystem number)

The number of digits entered in the PRIM PLUS SEC DIG STR field should be less than or equal to the total count specified for the parent translation group; each digit can be in the range 0-9. The subsystem number (DEST SS NUM field) is 0 if no subsystem is identified, or 2-225 for a unique reference.

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

2. Enter **i** to insert the data.
 - If "FORM INSERTED" flashes in the upper right corner of the screen, CONTINUE this procedure.
 - If the insert fails due to the fact that the maximum number of translations allowed for the parent translation group is insufficient, EXIT this procedure. Increase the PRIM PLUS SEC count for the parent translation group, using the procedure "Update SCCP Translation Group," Procedure 13.3.10, and then reenter this procedure.
 - If the insert fails due to the fact that the target DPC/destination system number is not a valid SCCP route for the target GSM, EXIT this procedure immediately. Use the procedure "Define Primary/Backup SCCP Route Destinations," Section 13.3.3, to define the missing routes before reentering this procedure.
3. Enter **<** to return to the forms menu and **q** to exit RC/V.
4. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

5. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.12: Define Single GTT with Fixed Digit String

OVERVIEW

This procedure defines an individual global title translation (GTT) with a **fixed** digit string, and, if needed, the GTT defining the number of translations associated with the target fixed digit string. The parent SCCP translation group must be defined.

Due to the potential complexity of the data entered, it is imperative that administrators have accurate translation data prepared in advance according to local practices, consulting 235-080-100, *5ESS®-2000 Switch Translation Guide (TG5)*.

Finally, any DPC/subsystem designated in a GTT must be provisioned as a primary or backup route destination on the target SCCP GSM.

PROCEDURE

1. Has a translation subgroup already been provisioned with the target fixed digit string?
 - If **yes**, SKIP to Step 3.
 - If **no**, CONTINUE this procedure.
2. At an RC/V terminal, enter **16.25i** to access the SCCP SINGLE GLOBAL TITLE TRANSLATION view in INSERT mode.

Enter the following data to establish a translation subgroup associated with a particular fixed string:

GSM	(target SCCP GSM number)
TRANS GROUP	(parent translation group)
FIX DIG STR	(see below)
PRIM PLUS SEC DIG STR	(leave this field blank)
MAX TRANS	(maximum number of translations for this fixed digit string)
DEST GSM	(blank)
DPC	(blank)
DEST SS NUM	(blank)

The number of fixed string digits (FIX DIG STR field) entered must correspond to the number specified for the parent translation group; each digit can be in the range 0-9. Also, the maximum number of translations associated with **all** SCCP translation groups combined is 131071.

SKIP to Step 4.

3. Is the number of maximum translations associated with the target fixed digit string sufficient to define as new GTT?
 - If **no**, use the procedure "Update Single GTT with Fixed Digit Strings," Procedure 13.3.14, to increase the maximum number of translations (MAX TRANS field) for the target fixed digit strings. Then CONTINUE this procedure.
 - If **yes**, CONTINUE this procedure.
4. At an RC/V terminal, enter **16.25i** to access the SCCP SINGLE GLOBAL TITLE TRANSLATION view in INSERT mode.

Enter the following data for the new GTT:

GSM	(target SCCP GSM number)
TRANS GROUP	(parent translation group)
FIX DIG STR	(target fixed digit string)
PRIM PLUS SEC DIG STR	(see below)
MAX TRANS	(leave blank)
DEST GSM	(target SCCP GSM number)
DPC	(9-digit primary/backup DPC)
DEST SS NUM	(primary/backup subsystem number)

The number of digits entered in the PRIM PLUS SEC DIG STR field should be less than or equal to the total count specified for the parent translation group (sum of NUM PRIM DIGITS plus NUM SEC DIGITS); each digit can be in the range 0-9. The subsystem number (DEST SS NUM field) is 0 if no subsystem is identified, or 2-225 for a unique subsystem.

When all data is entered, the string *Enter Insert, Validate, or Print:* is produced.

5. Enter **i** to insert the data.

- If "FORM INSERTED" flashes in the upper right corner of the screen, enter **<** to return to the forms menu and **q** to exit RC/V, and then CONTINUE this procedure.
- If the insert fails due to the fact that the maximum number of translations associated with the target fixed digit string is insufficient, RETURN to Step 3.
- If the insert fails due to the fact that the target DPC/destination system number is not a valid SCCP route for the target GSM, EXIT this procedure immediately. Use the procedure "Define Primary/Backup SCCP Route Destinations," Section 13.3.3, to define the missing routes before reentering this procedure.

6. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

7. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.13: Update Single GTT with Non-Fixed Digit String

OVERVIEW

This procedure updates an individual global title translation (GTT) with a **non-fixed** digit string.

Due to the potential complexity of the data entered, it is imperative that administrators have accurate translation data prepared in advance according to local practices, consulting 235-080-100, *5ESS®-2000 Switch Translation Guide (TG5)*.

Finally, any DPC/subsystem designated in a GTT must be provisioned as a primary or backup route destination on the target SCCP GSM.

PROCEDURE

1. At an RC/V terminal, enter **16.25u** to access the SCCP SINGLE TITLE TRANSLATION view in UPDATE mode.

Enter the following key data:

GSM	(target SCCP GSM number)
TRANS GROUP	(parent translation group)
FIX DIG STR	(leave blank)
PRIM PLUS SEC DIG STR	(target primary/secondary digit string)

The following additional fields will be populated:

MAX TRANS	(is blank - cannot be updated)
DEST GSM	(target SCCP GSM number - cannot be updated)
DPC	(current DPC route)
DEST SS NUM	(current subsystem number)

and the string *Enter Update, Change, Validate, or Print:* is produced.

2. Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the field to be changed (only DPC and DEST SS NUM can be updated) to move the cursor to that field. Continue until all desired fields are updated, and then enter **<** to return to the command line. The string *Enter Update, Change, Validate, or Print:* is produced.

3. Enter **u** to update the data.

- If "FORM UPDATED" flashes in the upper right corner of the screen, the update has completed successfully. CONTINUE the procedure.
- If the update fails due to the fact that the target DPC/destination system number is not a valid SCCP route for the target GSM, EXIT this procedure immediately. Use the procedure "Define Primary/Backup SCCP Route Destinations," Section 13.3.3, to define the missing routes before reentering this procedure.

4. Enter **<** to return to the forms menu and **q** to exit RC/V.
5. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

6. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.14: Update Single GTT with Fixed Digit String

OVERVIEW

This procedure updates an individual global title translation (GTT) using a **fixed** digit string.

Due to the potential complexity of the data entered, it is imperative that administrators have accurate translation data prepared in advance according to local practices, consulting 235-080-100, *5ESS®-2000 Switch Translation Guide (TG5)*.

Finally, any DPC/subsystem designated in a GTT must be provisioned as a primary or backup route destination on the target SCCP GSM.

PROCEDURE

- Is maximum number of translations associated with a particular fixed digit string (MAX TRANS field) to be updated?
 - If **yes**, CONTINUE this procedure.
 - If **no**, SKIP to Step 7.
- If MAX TRANS is being updated, then no primary/secondary digit string GTT can exist (use the procedure "Delete Single GTT with Fixed Digit Strings," Procedure 13.3.17), or SCCP must be in a GROW state (use the procedure "Deactivate Connectionless SCCP Processing," Procedure 13.3.21).
- At an RC/V terminal, enter **16.25u** to access the SCCP SINGLE GLOBAL TITLE TRANSLATION view in UPDATE mode.

Enter the following key data:

GSM	(target SCCP GSM number)
TRANS GROUP	(target translation group)
FIX DIG STR	(target fixed digit string)
PRIM PLUS SEC DIG STR	(leave blank)

The following additional fields are populated:

MAX TRANS	(current maximum number of translations)
DEST GSM	(blank)
DPC	(blank)
DEST SS NUM	(blank)

and the string *Enter Update, Change, Validate, or Print:* is produced.

- Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the MAX TRANS field to move the cursor there, and enter the new value. Enter **<** to return to the command line; the string *Enter Update, Change, Validate, Or Print:* is produced.

- Enter **u** to update the data.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen. Enter **<** to return to the forms menu.

6. Dependent upon the actions taken in Step 2, perform one of the following actions:
 - If all primary/secondary digit string GTTs were deleted, reinsert them with the procedure "Define Single GTT with Fixed Digit String," Procedure 13.3.12 .
 - If SCCP processing was deactivated, reactivate SCCP using the procedure "Begin SCCP Data Initialization, Procedure 13.3.7 .

Skip to Step 11.

7. At an RC/V terminal, enter **16.25u** to access the SCCP SINGLE GLOBAL TITLE TRANSLATION view in UPDATE mode.

Enter the following key data:

GSM	(target SCCP GSM number)
TRANS GROUP	(target translation group)
FIX DIG STR	(target fixed digit string)
PRIM PLUS SEC DIG STR	(target primary/secondary digit string)

The following additional fields will be populated:

MAX TRANS	(is blank - cannot be updated)
DEST GSM	(target SCCP GSM number - cannot be updated)
DPC	(current DPC route)
DEST SS NUM	(current subsystem number)

and the string *Enter Update, Change, Validate, or Print:* is produced.

8. Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the field to be changed (only DPC and DEST SS NUM can be updated) to move the cursor to that field. Continue until all desired fields are updated, and then enter **<** to return to the command line. The string *Enter Update, Change, Validate, or Print:* is produced.

9. Enter **u** to update the data.
 - If "FORM UPDATED" flashes in the upper right corner of the screen, the update has completed successfully. CONTINUE the procedure.
 - If the update fails due to the fact that the target DPC/destination system number is not a valid SCCP route for the target GSM, EXIT this procedure immediately. Use the procedure "Define Primary/Backup SCCP Route Destinations," Section 13.3.3 , to define the missing routes before reentering this procedure.
10. Enter **<** to return to the forms menu and **q** to exit RC/V.
11. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.
12. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.15: Update SCCP Translation Table

OVERVIEW

This procedure updates called party address treatment for a specific TCAP application.

In the 5E11 software release, this procedure is normally used to change the SCCP translation group (i.e., the GTT digit analysis) associated with a specific TCAP application. In the 5E12 software release, the procedure can also be used to convert from local to remote GTT digit analysis (or visa-versa), or to change the remote DPC to perform GTT functions.

PROCEDURE

1. What is the intent of this update?
 - If the intent is to *retain local* GTT digit analysis, and modify the translation group associated with a specific translation type (this is the only update allowed in the 5E11 software release), CONTINUE this procedure.
 - If the intent is to *convert local* to *remote* GTT digit analysis (allowed only in the 5E12 software release), SKIP to Step 5.
 - If the intent is to *retain remote* GTT digit analysis, and modify the remote DPC associated with a specific translation type (allowed only in the 5E12 software release), SKIP to Step 8.
 - If the intent is to *convert remote* to *local* GTT digit analysis (allowed only in the 5E12 software release), SKIP to Step 10.
2. At an RC/V terminal, enter **16.24u** to access the SCCP TRANSLATION TABLE view in UPDATE mode.

Enter the following key data:

GSM	(target SCCP GSM number)
TRANS TYPE	(translation type associated with the target TCAP application)

The following updatable fields will appear with current values:

TRANS GROUP	(current translation group)
START GTT DIGIT	(current digit to start analysis)

and the string *Enter Update, Change, Validate, or Print:* is produced. In the 5E12 software release, the field **DPC** will also be present (it should be blank in this case), but should not be changed by this procedural leg.

3. Enter **c** to start the change mode. The expected response is the *Change field:* string.

Enter the field number to move the cursor to that field and then enter the desired data. After the data is entered the *Change field:* prompt will reappear.

Repeat this step until all desired fields are changed.

When all changes are completed, enter **<** to access the main menu; the string *Enter Update, Change, Validate, or Print:* is produced.

4. Enter **u** to update the data.

- If "FORM UPDATED" flashes in the upper right corner of the screen, the update has completed successfully. Enter < to return to the forms menu and **q** to quit RC/V, and SKIP to Step 12.
 - If the update fails due to the fact that the target translation group is not defined on the GSM, EXIT this procedure immediately. Use the procedure "Define GTT Translation Groups with Non-Fixed Digit String," Section 13.3.4, or "Define GTT Translation Groups with Fixed Digit String," Section 13.3.5, to define the missing translation group, and then restart this procedure.
5. At an RC/V terminal, enter **16.24u** to access the SCCP TRANSLATION TABLE view in UPDATE mode, recalling the 5E12 software release is required to provision *remote GTT processing*.

Enter the following data:

GSM	(target SCCP GSM number)
TRANS TYPE	(translation type associated with the target TCAP application)

The following fields should be populated with current values:

TRANS GROUP	(current translation group)
START GTT DIGIT	(current digit to start analysis)
DPC	(should be blank)

and the string *Enter Update, Change, Validate, or Print:* is produced.

6. Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the *TRANS GROUP* field and *blank* it by entering an ' (apostrophe); repeat this action for the *START GTT DIGIT* field.

Next enter the number of the *DPC* field, and enter the number of the remote DPC slated to perform GTT processing.

Enter < to access the main menu. The string *Enter Update, Change, Validate, or Print:* is produced.

7. Enter **u** to update the data.

- If "FORM UPDATED" flashes in the upper right corner of the screen, the update has completed successfully. Enter < to return to the forms menu and **q** to exit RC/V, and SKIP to Step 12.
- If the update fails due to the fact that the target DPC is not a valid SCCP route for the target GSM, EXIT this procedure immediately. Use the procedure "Define Primary/Backup SCCP Route Destinations," Section 13.3.3, to define the missing routes before reentering this procedure.

8. At an RC/V terminal, enter **16.24u** to access the SCCP TRANSLATION TABLE view in UPDATE mode, recalling the 5E12 software release is required to provision *remote GTT processing*.

Enter the following data:

GSM	(target SCCP GSM number)
TRANS TYPE	(translation type associated with the target TCAP application)

The following fields should be populated with current values:

TRANS GROUP	(should be blank - do not change)
START GTT DIGIT	(should be blank - do not change)
DPC	(current DPC performing remote GTT processing)

and the string *Enter Update, Change, Validate, or Print:* is produced.

9. Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the *DPC* field, and enter the number of the new remote DPC slated to perform GTT processing.

Enter **<** to access the main menu. The string *Enter Update, Change, Validate, or Print:* is produced.

RETURN to Step 7.

10. At an RC/V terminal, enter **16.24u** to access the SCCP TRANSLATION TABLE view in UPDATE mode, recalling the 5E12 software release is required to provision *remote GTT processing*.

Enter the following data:

GSM	(target SCCP GSM number)
TRANS TYPE	(translation type associated with the target TCAP application)

The following fields should be populated with current values:

TRANS GROUP	(should be blank)
START GTT DIGIT	(should be blank)
DPC	(current DPC performing remote GTT processing)

and the string *Enter Update, Change, Validate, or Print:* is produced.

11. Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the *DPC* field and *blank* it by entering an ' (apostrophe).

Next enter the number of the *TRANS GROUP* field, and enter the number of the translation group to be used for local digit analysis; repeat this action for the **START GTT DIGIT** field to indicate the digit where analysis is to start.

Enter **<** to access the main menu. The string *Enter Update, Change, Validate, or Print:* is produced.

RETURN to Step 4.

12. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

13. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.16: Delete Single GTT with Non-Fixed Digit String

OVERVIEW

This procedure deletes one or more individual global title translations (GTTs) which use a **non-fixed** digit string.

PROCEDURE

1. Will the last GTT on an SCCP GSM be deleted by this procedure?
 - If **yes**, deactivate SCCP processing on that GSM, using the procedure "Deactivate Connectionless SCCP Processing," Procedure 13.3.21, before CONTINUING.
 - If **no**, CONTINUE this procedure.

2. Has all data, associated with the non-fixed digit string GTTs to be deleted, been identified?
 - If **yes**, SKIP to Step 4.
 - If **no**, CONTINUE this procedure.

3. Issue the input message:

OP:OFR,FORM=6015,DEVICE=xxx

on an MCC/STLWS to produce office records for the SCCP GLOBAL TITLE TRANSLATION view. The destination **xxx** is described in "SCCP Provisioning Overview," Procedure 13.3.

Survey the output to obtain pertinent data associated with the GTTs of interest (SCCP GSM number, translation group, primary plus secondary digit strings).

4. At an RC/V terminal, enter **16.25d** to access the SCCP SINGLE GLOBAL TITLE TRANSLATION view in DELETE mode.

Enter the following key data:

GSM	(target SCCP GSM number)
TRANS GROUP	(target translation group)
FIX DIG STR	(leave blank)
PRIM PLUS SEC DIG STR	(target primary plus secondary digit string)

The string *Enter Delete, Validate, or Print*: is produced.

5. Enter **d** to start the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

6. Are there more translations to be deleted?
 - If **yes**, RETURN to Step 4.
 - If **no**, CONTINUE this procedure.

7. Enter < to return to the forms menu and q to exit RC/V.
8. Back up the new ODD by entering the input message:
BKUP : ODD
on an MCC/STLWS.
9. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.17: Delete Single GTT with Fixed Digit String

OVERVIEW

This procedure deletes one or more individual global title translations (GTTs) which use a **fixed** digit string.

PROCEDURE

1. Will the last GTT on an SCCP GSM be deleted by this procedure?
 - If **yes**, deactivate SCCP processing on that GSM, using the procedure "Deactivate Connectionless SCCP Processing," Procedure 13.3.21, before CONTINUING.
 - If **no**, CONTINUE this procedure.

2. Has all data, associated with the fixed digit string GTTs to be deleted, been identified?
 - If **yes**, SKIP to Step 4.
 - If **no**, CONTINUE this procedure.

3. Issue the input message:

OP:OFR,FORM=6015,DEVICE=xxx

on an MCC/STLWS to produce office records for the SCCP GLOBAL TITLE TRANSLATION view. The destination **xxx** is described in "SCCP Provisioning Overview," Procedure 13.3.

Survey the output to obtain pertinent data associated with the GTTs of interest (SCCP GSM number, translation group, fixed digit string, primary plus secondary digit strings).

4. At an RC/V terminal, enter **16.25d** to access the SCCP SINGLE GLOBAL TITLE TRANSLATION view in DELETE mode.

Enter the following key data:

GSM	(target SCCP GSM number)
TRANS GROUP	(target translation group)
FIX DIG STR	(target fixed digit string)
PRIM PLUS SEC DIG STR	(target primary plus secondary digit string)

The string *Enter Delete, Validate, or Print:* is produced.

5. Enter **d** to start the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

6. Are there more translations to be deleted?
 - If **yes**, RETURN to Step 4.
 - If **no**, CONTINUE this procedure.

7. Have all primary plus secondary string GTTs associated with a fixed digit string been deleted?
 - If **yes**, CONTINUE this procedure.
 - If **no**, SKIP to Step 10.
8. Delete the GTT that defines the maximum number of translations for the target fixed digit by entering the following data:

GSM	(target SCCP GSM number)
TRANS GROUP	(target translation group)
FIX DIG STR	(fixed digit string)
PRIM PLUS SEC DIG STR	(leave blank)

The string *Enter Delete, Validate, or Print:* is produced.

9. Enter **d** to start the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.
10. Enter **<** to return to the forms menu and **q** to exit RC/V.
11. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.
12. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.18: Delete SCCP Translation Table

OVERVIEW

This procedure degrows an SCCP translation table. This effectively decouples a TCAP application (identified by the translation type) from a specific SCCP translation group.

PROCEDURE

1. First, determine if the **translation type** to be deleted is currently being used by any TCAP application.

Issue the input message:

OP:OFR,FORM=5537,DEVICE=xxx

on an MCC/STLWS to produce office records for the DIRECT SIGNALING APPLICATION view. The device **xxx** is described in "SCCP Provisioning Overview," Procedure 13.3 .

Note if the TRANS TYPE field matches the translation type of the SCCP translation table to be deleted.

— If there is **no** match, skip to Step 3.

— If a **match occurred**, record the corresponding TCAP application (APPLIC field), and CONTINUE this procedure.

2. Next, determine if the identified TCAP application uses the SCCP GSM signaling platform.

At an RC/V terminal, enter **8.42r** to access the CCS TCAP APPLICATION view in REVIEW mode.

Enter the key fields:

SM	(target SCCP GSM number)
APPLICATION	(TCAP application from Step 1)

The current value of the PLATFORM field will be populated (if the form is found).

— If the platform is **0** (CNI), or the form is not found (TCAP application is not defined for clients on the SCCP GSM), CONTINUE this procedure.

— If the platform is the **SCCP GSM number**, the TCAP application must now use a CNI platform (see "Change Signaling Platform for TCAP Applications," Procedure 13.5.2), or the TCAP application must be denied to clients on the SCCP GSM entirely (see "Delete Signaling Platform for TCAP Applications," Procedure 13.5.3), before CONTINUING this procedure.

3. At an RC/V terminal, enter **16.24d** to access the SCCP TRANSLATION TABLE view in DELETE mode.

Enter the following key data:

GSM	(target SCCP GSM number)
TRANS TYPE	(target translation type)

4. Enter **d** to start the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu and q to exit RC/V.

5. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

6. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.19: Delete SCCP Translation Group

OVERVIEW

This procedure will degrow an SCCP translation group. A successful deletion of an SCCP translation group requires that all child global title translations (GTTs) and the associated SCCP translation table be deleted first.

PROCEDURE

1. First, determine if the translation group to be deleted is used in any **SCCP translation table**.

Issue the input message:

OP:OFR,FORM=6014,DEVICE=xxx

on an MCC/STLWS, to produce office records for the SCCP TRANSLATION TABLE view. The device **xxx** is described in "SCCP Provisioning Overview," Procedure 13.3.

Note if the GSM and TRANS GROUP fields match the target GSM and translation group to be deleted.

- If there is **no** match, CONTINUE this procedure.
- If a **match occurred**, record the corresponding TRANS TYPE, and delete the parent translation table using the procedure "Delete SCCP Translation Table," Procedure 13.3.18, and then CONTINUE this procedure.

2. Next, determine if any **GTTs** are associated with the translation group to be deleted.

Issue the input message:

OP:OFR,FORM=6015,DEVICE=xxx

on an MCC/STLWS, to produce office records for the SCCP SINGLE GLOBAL TITLE TRANSLATION view. The device **xxx** is described in "SCCP Provisioning Overview," Procedure 13.3.

Note if any of the GTT's GSM and TRANS GROUP fields match the target GSM and translation group to be deleted.

- If there is **no** match, CONTINUE this procedure.
- If **any match** occurred, use the procedure "Delete Single GTT with Non-Fixed Digit String," Procedure 13.3.16, or "Delete Single GTT with Fixed Digit String," Procedure 13.3.17, as appropriate, to delete all GTTs associated with the target translation group. Then, CONTINUE this procedure.

3. At an RC/V terminal, enter **16.23d** to access the SCCP TRANSLATION GROUP MASK view in DELETE mode.

Enter the following key data:

GSM	(target SCCP GSM number)
TRANS GROUP	(target translation group number)

4. Enter **d** to start the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu and q to exit RC/V.

5. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

6. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.20: Delete Primary SCCP Route Destinations

OVERVIEW

This procedure will degrow a **primary** SCCP route destination. A successful deletion of an SCCP route requires the deletion of all GTTs referencing this route.

PROCEDURE

1. At an RC/V terminal, enter **16.22r** to access the SCCP PRIMARY/BACKUP DESTINATION view in REVIEW mode.

Enter the following key data:

GSM PRIMARY	(target SCCP GSM number)
DPC PRIMARY	(target 9-digit primary DPC)
SSN PRIMARY	(target primary subsystem number)

The following additional fields are populated:

GSM BACKUP	(blank or target SCCP GSM number)
DPC BACKUP	(blank or backup DPC)
SSN BACKUP	(blank or backup subsystem)

If the backup route is defined, it will still exist (after this procedure is completed) as a primary route destination, but the binding between the SCCP routes in this view will be broken. That primary route can be deleted by a separate execution of this procedure (if desired).

Enter < to return to the forms menu.

2. Next, determine if any **GTTs** are associated with the primary SCCP route destination to be deleted.

Issue the input message:

OP:OFR,FORM=6015,DEVICE=xxx

on an MCC/STLWS, to produce office records for the SCCP SINGLE GLOBAL TITLE TRANSLATION view. The device **xxx** is described in "SCCP Provisioning Overview," Procedure 13.3.

Note if any GTTs have DEST GSM, DPC, DEST SS NUM on the form match the GSM PRIMARY, DPC PRIMARY, SSN PRIMARY fields for the route to be deleted.

For **every** match, use the procedure "Delete Single GTT with Non-Fixed Digit String," Procedure 13.3.16, or "Delete Single GTT with Fixed Digit String," Procedure 13.3.17, as appropriate, to delete the GTTs. Alternately, the destination routes may be changed (use the procedure "Update Single GTT with Non-Fixed Digit String," Procedure 13.3.13, or "Update Single GTT with Fixed Digit String," Procedure 13.3.14). Then CONTINUE this procedure.

3. At an RC/V terminal, enter **16.22d** to access the SCCP PRIMARY/BACKUP DESTINATION view in DELETE mode.

Enter the following key data:

GSM PRIMARY	(target SCCP GSM number)
DPC PRIMARY	(target 9-digit primary DPC)
SSN PRIMARY	(target primary subsystem number)

4. Enter **d** to start the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

5. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

6. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.21: Deactivate Connectionless SCCP Processing

OVERVIEW

This procedure will deactivate the connectionless SCCP processing. This is necessary when certain SCCP translation updates are made, or when completely degrowing an SCCP GSM.

PROCEDURE

1. At an RC/V terminal, enter **16.21u** to access the SCCP PARAMETER DEFINITION view in UPDATE mode.

Specify the key field:

GSM	(target SCCP GSM number)

All the other fields are populated with current values, and the string *Enter Update, Change, Validate, or Print:* is produced.

2. Enter **c** to start the change mode. The expected response is the *Change field:* string.

Enter the number for the INIT STATUS field, and enter **GROW**. Enter the field number for the PROCESSING field, and enter **N** (for NO).

Enter **<** to return to the command line; the string *Enter Update, Change, Validate, or Print:* is produced.

3. Enter **u** to update the data.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu and **q** to exit RC/V.

4. Back up the new ODD by entering the input message:

BKUP:ODD

on an MCC/STLWS.

5. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.3.22: Delete Connectionless SCCP GSM

OVERVIEW

This procedure is used to completely undefine the SCCP capability on a target GSM.

To be successful, any SCCP route destinations, translation groups, translation tables, and GTTs associated with the target GSM must be deleted first.

PROCEDURE

1. Issue the input message:

OP:OFR,FORM=6013,DEVICE=xxx

on an MCC/STLWS, to produce office records for the SCCP TRANSLATION GROUP MASK view. The device **xxx** is described in "SCCP Provisioning Overview," Procedure 13.3. Note if the GSM field of any of the translation groups match the target GSM.

For every match found, use the procedure "Delete SCCP Translation Group," Procedure 13.3.19, to delete all translation groups associated with the target GSM. Then CONTINUE this procedure.

2. Issue the input message:

OP:OFR,FORM=6012,DEVICE=xxx

on an MCC/STLWS, to produce office records for the SCCP PRIMARY/BACKUP DESTINATION view. The device **xxx** is described in "SCCP Provisioning Overview," Procedure 13.3. Note if the GSM PRIMARY field of any of the SCCP route destinations match the target GSM.

For every match found, use the procedure "Delete Primary SCCP Route Destinations," Procedure 13.3.20, to delete all primary route destinations associated with the target GSM. Any backup route destinations will be deleted by this action. Then CONTINUE this procedure.

3. Issue the input message:

OP:CCS,SCMG,SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM number.

If any response **other than** "NG - SCCP NOT OPERATIONAL ON SM" appears in the output, use the procedure "Deactivate Connectionless SCCP Processing," Procedure 13.3.21, to place SCCP processing on the target GSM in a "growth" state.

4. At an RC/V terminal, enter **16.20d** to access the SCCP NETWORKS DEFINITION view in DELETE mode.

Enter the following key data:

GSM	(target SCCP GSM number)

The string *Enter Delete, Validate, or Print:* is produced.

5. Enter **d** to start the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu and q to exit RC/V.

6. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

7. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.4: MTP/SCCP MEASUREMENTS PROVISIONING

OVERVIEW

Measurement collection selectivity provide switch personnel with the ability to customize the collection of certain traffic measurements on a per office basis. Through the use of RC/V, selected measurements can be collected in a fixed amount of administrative module (AM) buffer space. Introduced in the 5E12 software release, the MTP/SCCP measurements associated with global switching modules (GSMs) allow this selectivity. This section describes the associated provisioning procedures.

See Table 13.4-1 for a list of RC/V views involved.

Table 13.4-1 MTP/SCCP Measurements Collection RC/V Views

VIEW	TITLE	USE	PURPOSE
13.7	MEASUREMENT COLLECTION SELECTIVITY	ru	Select/deselect individual measurement for collection or printing
13.8	MEASUREMENT RANGE SELECTIVITY	ru	Select/deselect range of measurements for collection or printing
13.9	MEASUREMENT COLLECTION SUMMARY	r	Review collection status of individual measurements
Note: The USE column indicates how the view is used: r for REVIEW and u for UPDATE.			

Define measurement selectivity using the procedures listed in Table 13.4-2.

Table 13.4-2 Define MTP/SCCP Measurement Collection on GSMs

JOB DESCRIPTION	PROCEDURE
Define signaling link (CCSLK) measurement collection	Procedure 13.4.1
Define signaling collection control part (SCCP) measurement collection	Procedure 13.4.2
Define destination point code (DPC) measurement collection	Procedure 13.4.3

The remainder of this section provides the specific procedures to define MTP/SCCP measurement collection for offices with GSMs. These procedures make no decisions about the selection of individual CCSLKs, SCCP platforms or DPCs for which measurements are to be collected or printed.

All of the procedures require access to RC/V views. This is accomplished by the choice of the **196** menu selection, or the input message, **rcv:menu:apprc** on an MCC/STLWS. Alternately, the input message **apprc** can be used on a **UNIX®/RC** terminal.

Consult local practices and 235-118-2xx, *5ESS®-2000 Switch Recent Change Reference* or 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)* for detailed descriptions of RC/V fields.

The MTP/SCCP measurements provisioning procedures in this section are:

PROCEDURE

1. Procedure 13.4.1 - CCSLK Measurement Collection Selection
2. Procedure 13.4.2 - SCCP Measurement Collection Selection
3. Procedure 13.4.3 - DPC Measurement Collection Selection

Procedure 13.4.1: CCSLK Measurement Collection Selection

OVERVIEW

This procedure allows switch personnel to control the collection or printing of 30-minute traffic (TRFC30) reports, Section 230 for individual or ranges of GSM signaling links (CCSLKs).

It is assumed that choices of CCSLKs to be provisioned are determined before entering this procedure. In addition to CCSLK numbers, personnel must know whether or not to collect a particular measurement and have it printed on the read-only printer (ROP).

PROCEDURE

1. For each CCSLK measurement to be provisioned, determine the current collection and printing status. At an RC/V terminal, enter **13.9** to access the MEASUREMENT COLLECTION SUMMARY view in REVIEW mode.

Enter the following data for a selected CCSLK:

SECTION NAME	(enter SL)
START1COMP	(target link set number)
START2COMP	(target link set member number)
START3COMP	(blank)
DEST SM	(target GSM number)

If "FORM NOT FOUND" flashes in the upper right corner of the screen, the specified CCSLK measurement is **not** currently being collected.

If the form is found, the specified CCSLK measurement is being collected and the ROP field will be populated with **N** if no printing to the ROP is scheduled, or **Y** if printing is the default.

Repeat this procedure for all CCSLKs identified and then enter < to return to the forms menu.

If the measurement collection or printing attributes are different than intended for any CCSLK, CONTINUE this procedure.

2. Determine the individual CCSLK or ranges of CCSLKs whose measurement's collection or printing characteristics are to be altered.
 - If the characteristics of **individual** CCSLK measurements are to be altered, CONTINUE this procedure.
 - If the characteristics of measurements of a **range** of CCSLKs are to be altered, SKIP to Step 6.
3. At an RC/V terminal, enter **13.7u** to access the MEASUREMENT COLLECTION SELECTIVITY view in UPDATE mode.

Enter the following key field data for the selected CCSLK:

SECTION NAME	(enter SL)
START1COMP	(target link set number)
START2COMP	(target link set member number)
START3COMP	(blank)
DEST SM	(target GSM number)

The following read-only fields will be populated:

- SPACE AVL. Displays the amount of memory available in the EADAS buffer (a zero or negative value indicates **no** new measurements should be provisioned for collection).
- PRT MSG UNIT AVL. Displays the number of message units available for printing on the ROP (a zero or negative value indicates **no** new measurements should be provisioned for printing).

Even if space is available, it may not be sufficient for collection or printing of new measurements, and the update will **fail**.

On screens 2 through 4, up to 54 collection components are listed, specifically listed CCSLKs starting with the CCSLK specified by key fields (or the first provisioned CCSLK thereafter). The ID column has two comma-separated numbers corresponding to a CCSLK's link set and member numbers, respectively. The COLLECT column indicates whether or not that CCSLK's measurement is being collected (Y for YES, N for NO), and the ROP column indicates whether or not that CCSLK's measurement is to be printed on the ROP with other TRFC30 measurements.

The string *Enter Update, Change, Validate, Screen #, or Print:* is produced.

4. Enter **c** to start change mode. The expected response is the *Change field:* string; enter the number of the COMPONENT COLLECTION LIST (CCL) field on screen 2, which results in the response *Row:*. Enter the **row number** of the measurement whose collection or printing attributes are to be changed.

Enter **Y** or **N** as appropriate, for the COLLECT and ROP fields associated with the measurement selected. Note that the measurement must be collected if ROP printing is desired.

If other measurements to be updated appear on any of the rows displayed, repeat the previous procedure.

5. Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen.

Enter **<** to return to the forms menu, and SKIP to Step 9.

6. At an RC/V terminal, enter **13.8u** to access the MEASUREMENT RANGE SELECTIVITY view in UPDATE mode.

Enter the following key field data for a selected range of CCSLKs:

SECTION NAME	(enter SL)
START1COMP	(beginning link set number of range)
START2COMP	(beginning link member number of range)
START3COMP	(blank)
END1COMP	(ending link set number of range)
END2COMP	(ending link member number of range)
END3COMP	(blank)
DEST SM	(target GSM number)

The following read-only fields will be populated:

- SPACE AVL. Displays the amount of memory available in the EADAS buffer (a zero or negative value indicates **no** new measurements should be provisioned for collection).
- PRT MSG UNIT AVL. Displays the number of message units available for printing on the ROP (a zero or negative value indicates **no** new measurements should be provisioned for printing).

Even if space is available, it may not be sufficient for collection or printing of new measurements, and the update will **fail**.

The COLLECT and ROP fields are blank at this point.

The string *Enter Update, Change, Validate, or Print:* is produced.

7. Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the COLLECT field, and enter **Y** to allow collection, or **N** to disallow collection.

If collection is allowed, ROP printing can be specified. If desired, enter the number of the ROP field, and enter **Y** to allow printing, or **N** to inhibit printing. A **blank** entry will preserve current ROP printing status for individual collected components.

It should be noted that **all** measurements in the **range** specified by the key fields will be impacted by this action.

8. Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen. Enter **<** to return to the forms menu, and CONTINUE this procedure.

9. Have the measurement collection or printing attributes for all identified CCSLKs been updated?

— If **yes**, CONTINUE this procedure.

— If **no**, RETURN to Step 2 to process changes for other CCSLKs.

10. Enter **q** to exit RC/V.

Back up the new ODD by entering the input message:

BKUP:ODD

on an MCC/STLWS.

11. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.4.2: SCCP Measurement Collection Selection

OVERVIEW

This procedure allows switch personnel to control the collection or printing of 30-minute traffic (TRFC30) reports, Section 233 for individual or ranges of signaling connection control part (SCCP) functionality on GSMs.

It is assumed that choices of GSMs to be provisioned are determined before entering this procedure. In addition to GSM numbers, personnel must know whether or not to collect a particular measurement and have it printed on the read-only printer (ROP).

PROCEDURE

1. For each SCCP measurement to be provisioned, determine the current collection and printing status. At an RC/V terminal, enter **13.9** to access the MEASUREMENT COLLECTION SUMMARY view in REVIEW mode.

Enter the following data for a selected SCCP GSM:

SECTION NAME	(enter SCCP)
START1COMP	(target GSM number)
START2COMP	(blank)
START3COMP	(blank)
DEST SM	(blank)

If "FORM NOT FOUND" flashes in the upper right corner of the screen, the SCCP measurement for the specified GSM is **not** currently being collected.

If the form is found, the SCCP measurement for the specified GSM is being collected, and the ROP field will be populated with **N** if no printing to the ROP is scheduled, or **Y** if printing is the default.

Repeat this procedure for all GSMs identified, and then enter < to return to the forms menu.

If the measurement collection or printing attributes are different than intended for any GSM, CONTINUE this procedure.

2. Determine the individual GSM or ranges of GSMs whose SCCP measurement's collection or printing characteristics are to be altered.
 - If the characteristics of SCCP measurements on **individual** GSMs are to be altered, CONTINUE this procedure.
 - If the characteristics of SCCP measurements of a **range** of GSMs are to be altered, SKIP to Step 6.
3. At an RC/V terminal, enter **13.7u** to access the MEASUREMENT COLLECTION SELECTIVITY view in UPDATE mode.

Enter the following key field data for the selected GSM whose SCCP measurement attributes are to change:

SECTION NAME	(enter SCCP)
START1COMP	(target GSM number)
START2COMP	(blank)
START3COMP	(blank)
DEST SM	(blank)

The following read-only fields will be populated:

- SPACE AVL. Displays the amount of memory available in the EADAS buffer (a zero or negative value indicates **no** new measurements should be provisioned for collection).
- PRT MSG UNIT AVL. Displays the number of message units available for printing on the ROP (a zero or negative value indicates **no** new measurements should be provisioned for printing).

Even if space is available, it may not be sufficient for collection or printing of new measurements, and the update will **fail**.

On screens 2 through 4, up to 54 collection components are listed, specifically provisioned GSMs, starting with the GSM specified by the key field (or the first provisioned GSM thereafter). The ID column is the GSM number, the COLLECT column indicates whether or not that SCCP measurement is being collected (Y for YES, N for NO), and the ROP column indicates whether or not that SCCP measurement is to be printed on the ROP with other TRFC30 measurements.

The string *Enter Update, Change, Validate, Screen #, or Print:* is produced.

4. Enter **c** to start change mode. The expected response is the *Change field:* string; enter the number of the COMPONENT COLLECTION LIST (CCL) field on screen 2, which results in the response *Row:*. Enter the **row number** of the measurement whose collection or printing attributes are to be changed.

Enter **Y** or **N** as appropriate, for the COLLECT and ROP fields associated with the measurement selected. Note that the measurement must be collected if ROP printing is desired.

If other measurements to be updated appear on any of the rows displayed, repeat the previous procedure.

5. Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen. Enter **<** to return to the forms menu, and **SKIP** to Step 8.

6. At an RC/V terminal, enter **13.8u** to access the MEASUREMENT RANGE SELECTIVITY view in UPDATE mode.

Enter the following key field data for a selected range of GSMs for which SCCP measurement attributes are to be modified:

SECTION NAME	(enter SCCP)
START1COMP	(beginning GSM number of range)
START2COMP	(blank)
START3COMP	(blank)
END1COMP	(ending GSM number of range)
END2COMP	(blank)
END3COMP	(blank)
DEST SM	(blank)

The following read-only fields will be populated:

- SPACE AVL. Displays the amount of memory available in the EADAS buffer (a zero or negative value indicates **no** new measurements should be provisioned for collection).
- PRT MSG UNIT AVL. Displays the number of message units available for printing on the ROP (a zero or negative value indicates **no** new measurements should be provisioned for printing).

Even if space is available, it may not be sufficient for collection or printing of new measurements, and the update will **fail**.

The COLLECT and ROP fields are blank at this point.

The string *Enter Update, Change, Validate, or Print:* is produced.

7. Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the COLLECT field, and enter **Y** to allow collection, or **N** to disallow collection.

If collection is allowed, ROP printing can be specified. If desired, enter the number of the ROP field, and enter **Y** to allow printing, or **N** to inhibit printing. A **blank** entry will preserve current ROP printing status for individual collected components.

It should be noted that **all** measurements in the **range** specified by the key fields will be impacted by this action.

8. Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen. Enter **<** to return to the forms menu, and CONTINUE this procedure.

9. Have the SCCP measurement collection or printing attributes for all identified GSMs been updated?

— If **yes**, CONTINUE this procedure.

— If **no**, RETURN to Step 2 to process changes for other GSMs.

10. Enter **q** to exit RC/V.

Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

11. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.4.3: DPC Measurement Collection Selection

OVERVIEW

This procedure allows switch personnel to control the collection or printing of 30-minute traffic (TRFC30) reports, Section 234 for individual or ranges of destination point codes (DPCs) on a given GSM.

It is assumed that choices of DPCs to be provisioned are determined before entering this procedure. In addition to DPC numbers, personnel must know whether or not to collect a particular measurement and have it printed on the read-only printer (ROP).

PROCEDURE

1. For each DPC measurement to be provisioned, determine the current collection and printing status. At an RC/V terminal, enter **13.9** to access the MEASUREMENT COLLECTION SUMMARY view in REVIEW mode.

Enter the following data for a selected SCCP GSM:

SECTION NAME	(enter PC)
START1COMP	(target 9-digit DPC)
START2COMP	(blank)
START3COMP	(blank)
DEST SM	(target GSM number)

If "FORM NOT FOUND" flashes in the upper right corner of the screen, the measurement for the specified DPC is **not** currently being collected.

If the form is found, the measurement for the specified DPC is being collected, and the ROP field will be populated with **N** if no printing to the ROP is scheduled, or **Y** if printing is the default.

Repeat this procedure for all DPCs identified, and then enter < to return to the forms menu.

If the measurement collection or printing attributes are different than intended for any DPC, CONTINUE this procedure.

2. Determine the individual DPC or ranges of DPCs whose measurement's collection or printing characteristics are to be altered.
 - If the characteristics of measurements for **individual** DPCs are to be altered, CONTINUE this procedure.
 - If the characteristics of measurements of a **range** of DPCs are to be altered, SKIP to Step 6.
3. At an RC/V terminal, enter **13.7u** to access the MEASUREMENT COLLECTION SELECTIVITY view in UPDATE mode.

Enter the following key field data for the selected DPC whose measurement attributes are to change:

SECTION NAME	(enter PC)
START1COMP	(target 9-digit DPC number)
START2COMP	(blank)
START3COMP	(blank)
DEST SM	(target GSM number)

The following read-only fields will be populated:

- SPACE AVL. Displays the amount of memory available in the EADAS buffer (a zero or negative value indicates **no** new measurements should be provisioned for collection).
- PRT MSG UNIT AVL. Displays the number of message units available for printing on the ROP (a zero or negative value indicates **no** new measurements should be provisioned for printing).

Even if space is available, it may not be sufficient for collection or printing of new measurements, and the update will **fail**.

On screens 2 through 4, up to 54 collection components are listed, specifically provisioned DPCs, starting with the DPC specified by the key field (or the first provisioned DPC thereafter). The ID column is the DPC number on the target GSM, the COLLECT column indicates whether or not that DPC measurement is being collected (Y for YES, N for NO), and the ROP column indicates whether or not that DPC measurement is to be printed on the ROP with other TRFC30 measurements.

The string *Enter Update, Change, Validate, Screen #, or Print:* is produced.

4. Enter **c** to start change mode. The expected response is the *Change field:* string; enter the number of the COMPONENT COLLECTION LIST (CCL) field on screen 2, which results in the response *Row:*. Enter the **row number** of the measurement whose collection or printing attributes are to be changed.

Enter **Y** or **N** as appropriate, for the COLLECT and ROP fields associated with the measurement selected. Note that the measurement must be collected if ROP printing is desired.

If other measurements to be updated appear on any of the rows displayed, repeat the previous procedure.

5. Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen. Enter **<** to return to the forms menu, and **SKIP** to Step 8.

6. At an RC/V terminal, enter **13.8u** to access the MEASUREMENT RANGE SELECTIVITY view in UPDATE mode.

Enter the following key field data for a selected range of DPCs on a specified GSM, for which measurement attributes are to be modified:

SECTION NAME	(enter PC)
START1COMP	(beginning 9-digit DPC in range)
START2COMP	(blank)
START3COMP	(blank)
END1COMP	(ending 9-digit DPC in range)
END2COMP	(blank)
END3COMP	(blank)
DEST SM	(target GSM number)

The following read-only fields will be populated:

- SPACE AVL. Displays the amount of memory available in the EADAS buffer (a zero or negative value indicates **no** new measurements should be provisioned for collection).
- PRT MSG UNIT AVL. Displays the number of message units available for printing on the ROP (a zero or negative value indicates **no** new measurements should be provisioned for printing).

Even if space is available, it may not be sufficient for collection or printing of new measurements, and the update will **fail**.

The COLLECT and ROP fields are blank at this point.

The string *Enter Update, Change, Validate, or Print:* is produced.

7. Enter **c** to start change mode. The expected response is the *Change field:* string.

Enter the number of the COLLECT field, and enter **Y** to allow collection, or **N** to disallow collection.

If collection is allowed, ROP printing can be specified. If desired, enter the number of the ROP field, and enter **Y** to allow printing, or **N** to inhibit printing. A **blank** entry will preserve current ROP printing status for individual collected components.

It should be noted that **all** measurements in the **range** specified by the key fields will be impacted by this action.

8. Enter **<** to return to the update command line and **u** to complete the update.

When the update completes, "FORM UPDATED" flashes in the upper right corner of the screen. Enter **<** to return to the forms menu, and CONTINUE this procedure.

9. Have the measurement collection or printing attributes for all identified DPCs been updated?

— If **yes**, CONTINUE this procedure.

— If **no**, RETURN to Step 2 to process changes for other DPCs.

10. Enter **q** to exit RC/V.

Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

11. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.5: TCAP APPLICATION PLATFORM PROVISIONING

OVERVIEW

In the 5E12 software release, clients on a specific SM subscribing to specific transaction capabilities application part (TCAP) applications can use the SS7 signaling platform resident on the *same* SM for transport, as an alternative to the office's common network interface (CNI) platform. It should be reiterated that TCAP clients must reside on a global switching module (GSM) to use its PSU-based signaling platform. In 5ESS®-2000 switch VCDX environments, all available TCAP services must be provisioned to use the resident PSU platforms. This section describes the associated provisioning procedures.

See Table 13.5-1 for the RC/V views involved.

Table 13.5-1 TCAP Signaling Platform Definition RC/V Views

VIEW	TITLE	USE	PURPOSE
8.17	DIRECT SIGNALING APPLICATION	r	Define TCAP application in office
8.42	CCS TCAP APPLICATION	riud	Define signaling platform for TCAP application
16.24	SCCP TRANSLATION TABLE	r	Verify SCCP translation group's existence

Note: The USE column indicates how the view is used: r for REVIEW, i for INSERT, u for UPDATE, and d for DELETE.

Table 13.5-2 specifies the procedures to designate the SS7 signaling platform for calls originating on a specific SM requiring a specific TCAP application.

Table 13.5-2 Designate Signaling Platform for TCAP Applications

JOB DESCRIPTION	PROCEDURE
Define signaling platform for TCAP application	Procedure 13.5.1
Change signaling platform for TCAP application	Procedure 13.5.2
Delete signaling platform for TCAP application	Procedure 13.5.3

Not all TCAP applications available in a 5ESS®-2000 switch office can use a GSM signaling platform, nor are all available in a 5ESS®-2000 switch VCDX environment, as enumerated in Table 13.5-3.

Table 13.5-3 TCAP Application Availability

TCAP APPLICATION	SWITCH SM ^a	SWITCH GSM ^b	VCDX ^b
ACND - Analog Calling Name Delivery	YES	YES	YES
AILS - Automated Inward Line Screening	YES	NO	NO
AINR0D1 - Advanced Services Platform Release 0.1	YES	YES	YES
APSDN - Software Defined Network at an Action Point	YES	NO	NO
ASP - Advanced Services Platform Release 0.0	YES	YES	NO
ASP - Advanced Services Platform Release 0.0B	YES	YES	YES
ATI - ANS® TCAP Type 1	YES	NO	NO
CCS7 - Common Channel Signaling System 7 TCAP	YES	NO	NO
DCIS - Destination Routed CCIS6	YES	NO	NO
ICCV - International Credit Card Validation	YES	NO	NO
ISVM - Inter-Switch Voice Messaging	YES	YES	YES
LALT - LIDB Alternate Destination	YES	NO	NO
LASS - Local Area Signaling Services	YES	YES	YES
LIDB - Line Information Data Base	YES	NO	NO
LNACP - Lease Network Action Control Point	YES	NO	NO
NS800 - Number Service 800 Application	YES	YES	YES
ONAI - OSPS Network Access Interrupt Application	YES	NO	NO

TNAI - Toll Network Access Interrupt Application	YES	NO	NO
Notes:			
a. CNI Platform			
b. GSM Platform			

The remainder of this section provides specific procedures to define TCAP application signaling platforms. The procedures provide information only on the new assignment of signaling platforms; they do not provide information about the selection or provisioning of particular TCAP applications in an office.

It should be noted that retrofit to the 5E12 software release will cause the ODD to be evolved, such that 5ESS®-2000 switch offices will have the CNI signaling platform defined for all provisioned TCAP applications on all SMs, and VCDX offices will have the GSM platform defined. Also, if a **new** TCAP application is **inserted** using the **8.17 DIRECT SIGNALING APPLICATION** view, TCAP application platform data will be inserted automatically as follows:

- If the office is equipped with a **CNI**, default data will be populated for every SM/SM-2000 indicating the CNI will be used as the TCAP application signaling platform. The procedure in "Change Signaling Platform for TCAP Applications," Procedure 13.5.2, can be used to specify a GSM platform.
- If the office is **not** equipped with a **CNI**, default data will be populated for every **GSM** indicating the PSU platform will be used for signaling for that TCAP application (if SCCP is available for that TCAP application's translation type).

Finally, if a TCAP application is **deleted** from the office using the **8.17 DIRECT SIGNALING APPLICATION** view, TCAP application platform data will be deleted automatically on all SM/SM-2000s.

All of the procedures require access to RC/V views. This is accomplished by the choice of the **196** menu selection, or the input message, **rcv:menu:apprc** on an MCC/STLWS. Alternately, the input message **apprc** can be used on a **UNIX®/RC** terminal.

Consult local practices and 235-118-2xx, *5ESS®-2000 Switch Recent Change Reference* or 235-080-100, *5ESS®-2000 Switch Translation Guide (TG-5)* for detailed descriptions of RC/V fields.

The TCAP application platform provisioning procedures in this section are:

PROCEDURE

1. Procedure 13.5.1 - Define Signaling Platform for TCAP Applications
2. Procedure 13.5.2 - Change Signaling Platform for TCAP Applications
3. Procedure 13.5.3 - Delete Signaling Platform for TCAP Applications

Procedure 13.5.1: Define Signaling Platform for TCAP Applications

OVERVIEW

This procedure allows the definition of a signaling platform for lines terminating on a specific SM, using a specific transactions capability application part (TCAP) application.

It is assumed that the identified TCAP application is already defined in the office, but has *not* yet been assigned a signaling platform for the client on the specified SM. This should only occur during SM/SM-2000 growth.

PROCEDURE

1. Verify that the target TCAP application has been defined in the office, by entering **8.17r** on an RC/V terminal to access the DIRECT SIGNALING APPLICATION view in REVIEW mode.

Enter the target TCAP application in the key field (selected from the entries in Table 13.5-3):

APPLIC	(target TCAP application)

- If "FORM NOT FOUND" flashes in the upper right corner of the screen, this procedure is not appropriate. EXIT this procedure immediately and provision the target TCAP application according to local practices.
- Otherwise, note the value of the TRANS TYPE field, enter < to return to the forms menu, and CONTINUE this procedure.

2. Is the intent of this procedure to assign a **GSM signaling platform** for the target TCAP application?

- If **yes**, CONTINUE this procedure.
- If **no**, SKIP to Step 4.

3. Determine if the target SM is a GSM which has SCCP available with the target TCAP application's translation type.

Enter **16.24r** on an RC/V terminal to access the SCCP TRANSLATION TABLE view in REVIEW mode.

Enter the following key fields:

GSM	(target GSM number)
TRANS TYPE	(derived from 8.17 view in Step 1)

- If "FORM NOT FOUND" flashes in the upper right corner of the screen, this procedure is not appropriate. EXIT this procedure immediately, and provision the required SCCP translation type for the GSM using "Define SCCP Translation Table," Procedure 13.3.6.
- Otherwise, CONTINUE this procedure.

4. At an RC/V terminal, enter **8.42i** to access the CCS TCAP APPLICATION view in INSERT mode.

Enter the following fields:

SM	(target SM)

APPLICATION	(target TCAP application)
PLATFORM	(0 for CNI or target SM number for GSM platform)

The string *Enter Insert, Validate, or Print:* is produced.

5. Enter i to complete the insert.

Evaluate the output:

- If "DUPLICATE FORM" flashes in the upper right corner of the screen, enter < to return to the forms menu and **q** to exit RC/V. EXIT this procedure immediately, as clients on the target SM already have a signaling platform designated, and execute the procedure "Change Signaling Platform for TCAP Applications," Procedure 13.5.2, to change platforms, if desired.
- If "FORM INSERTED" flashes in the upper right corner of the screen, enter < to return to the forms menu and **q** to exit RC/V. CONTINUE this procedure.

6. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

7. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.5.2: Change Signaling Platform for TCAP Applications

OVERVIEW

This procedure allows switch personnel to change the signaling platform for lines terminating on a specific SM, using a specific transaction capability application part (TCAP) application.

PROCEDURE

1. Is the intent of this procedure to change the signaling platform **from CNI to a GSM** for the target application?
 - If **yes**, CONTINUE this procedure.
 - If **no**, SKIP to Step 4.
2. Verify that the target TCAP application has been defined in the office, by entering **8.17r** on an RC/V terminal to access the DIRECT SIGNALING APPLICATION view in REVIEW mode.

Enter the target TCAP application in the key field (selected from the entries in Table 13.5-3):

APPLIC	(target TCAP application)

- If "FORM NOT FOUND" flashes in the upper right corner of the screen, this procedure is not appropriate. EXIT this procedure immediately and provision the target TCAP application according to local practices.
- Otherwise, note the value of the TRANS TYPE field, enter < to return to the forms menu, and CONTINUE this procedure.

3. Determine if the target SM is a GSM which has SCCP available with the target TCAP application's translation type.

Enter **16.24r** on an RC/V terminal to access the SCCP TRANSLATION TABLE view in REVIEW mode.

Enter the following key fields:

GSM	(target GSM number)
TRANS TYPE	(derived from 8.17 view in Step 1)

- If "FORM NOT FOUND" flashes in the upper right corner of the screen, this procedure is not appropriate. EXIT this procedure immediately, and provision the required SCCP translation type for the GSM using "Define SCCP Translation Table," Procedure 13.3.6.
- Otherwise, CONTINUE this procedure.

4. At an RC/V terminal, enter **8.42u** to access the CCS TCAP APPLICATION view in UPDATE mode.

Enter the key fields:

SM	(target SM number)
APPLICATION	(target TCAP application)

Evaluate the output:

- If "FORM NOT FOUND" flashes in the upper right corner of the screen, enter < to return to the forms menu and **q** to exit RC/V. EXIT this procedure immediately, as a signaling platform to support clients on the target SM with the specified TCAP application has not yet been defined, and therefore, cannot be changed. Execute the procedure "Define Signaling Platform for TCAP Applications," Procedure 13.5.1, to define a new platform, if desired.
- Otherwise, the PLATFORM field is populated with its current value, and the string *Enter Update, Change, Validate, or Print:* is produced. CONTINUE this procedure.

5. Enter **c** to start change mode. The expected response is the *Change field:* string. Enter the number of the PLATFORM field to be updated to move the cursor to that field; enter **0** for a CNI platform, or the **target SM number** for a GSM platform.

Enter < to return to the command line and **u** to complete the update. When "FORM UPDATED" flashes in the upper right corner of the screen, enter < to return to the forms menu and **q** to exit RC/V.

6. Back up the new ODD by entering the input message:

BKUP : ODD

on an MCC/STLWS.

7. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 13.5.3: Delete Signaling Platform for TCAP Applications

OVERVIEW

This procedure allows switch personnel to undefine a specific TCAP application from all clients on an identified SM. This should only be necessary during SM/SM-2000 degrowth.

PROCEDURE

1. At an RC/V terminal, enter **8.42d** to access the CCS TCAP APPLICATION view in DELETE mode.

Enter the following key fields:

SM	(target SM number)
APPLICATION	(target TCAP application).

Evaluate the output:

- If "FORM NOT FOUND" flashes in the upper right corner of the screen, enter < to return to the forms menu and **q** to exit RC/V. EXIT this procedure immediately, as there is no signaling platform for the target TCAP application for clients on the target SM.
- Otherwise, the string *Enter Update, Delete, Validate, or Print:* is produced. CONTINUE this procedure.

2. Enter **d** to complete the deletion process.

When the deletion completes, "FORM DELETED" flashes in the upper right corner of the screen.

Enter < to return to the forms menu and **q** to exit RC/V.

3. Back up the new ODD by entering the input message:

BKUP:ODD

on an MCC/STLWS.

4. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

14. SS7 - PSU MAINTENANCE CONSIDERATIONS

Procedure 14.1: PROBLEM ANALYSIS STRATEGIES

OVERVIEW

When CCS network faults occur on a global switching module (GSM), maintenance software automatically attempts to recover from the failure or at least minimize the impact on system operation. If problems cannot be corrected, associated hardware units or CCS signaling links (CCSLKs) or a message delivery (MD) link may be left in some off-normal condition that requires maintenance personnel intervention. The procedures in this section provide a guide to analyze these problems.

These procedures also identify cases where, maintenance personnel may have removed an associated hardware unit/CCSLK or inhibited/blocked a CCSLK when the system was operating under different conditions, and now it may be appropriate to return those units to full service.

If the administrative module (AM) is rolling in initializations, or the GSM is isolated from the AM, it's not possible to repair CCS-related problems, until AM-SM communications is restored; see the "System Recovery" section of the 235-120-120, *5ESS®-2000 Switch Very Compact Digital Exchange User's Guide*, to resolve these communications problems on a VCDX, or 235-105-250, *System Recovery*, to resolve problems on a general 5ESS®-2000 switch SM/SM-2000.

GSM isolation, by itself, does not mean that CCS functionality has been compromised. Access to the CCS network is based upon a PSU platform contained entirely within the SM, and call processing uses SM-local hunting algorithms (if stand-alone call processing is provisioned). CCS operation can be fully functional, even when the GSM is isolated.

Even reports of CCS trouble received prior to entering SM stand-alone operation may have "self-corrected" due to autonomous recovery procedures. In any event, AM-SM communications must be restored **first**, before attempting to manually resolve CCS problems.

GSM CCS problems are identified by various sources/techniques. The following sections describes three problem analysis strategies and seven step-by-step procedures to clear specific problems.

For each of the problem identification strategies, a suggested sequence of resolution/repair is implied based upon the importance of hardware units/CCSLKs to CCS operation, or parent/child relationships of hardware/CCSLKs. If another sequence is used, the individual procedures may still be successful. Instructions are provided to use alternate procedures, such as recovering parent hardware before a child is made operational.

The problem analysis procedures in this section are:

PROCEDURE

1. Procedure 14.1.1 - Analysis of Asynchronous Error Reports
2. Procedure 14.1.2 - Analysis Using MCC Indicators
3. Procedure 14.1.3 - Analysis Using Off-Normal Status

Procedure 14.1.1: Analysis of Asynchronous Error Reports

OVERVIEW

This strategy concerns CCS network failures on a GSM detected by recovery software. If an error is addressed by fault recovery, **REPT CCSLK**, **REPT MD**, **REPT CCS APC**, and/or **REPT CCS DPC** alarmed messages are produced. Similar unalarmed messages are produced when the cause of the removal was manually initiated, such as a CCSLK manual deactivation (**RMV:CCSLK**).

In the REPT messages, affected CCSLKs/DPCs may be identified or further investigation may be necessary to identify candidates for repair, and "error classes" may be identifiable by specific phrases listed in this procedure. The procedure points to the appropriate problem clearing procedure, based upon the CCS entity/error class identified. If multiple REPT messages implicate different CCS entities/error types/alarm levels, resolution of problems should follow the order in the following list.

NOTE: A **REPT**: output message indicates a problem has occurred some time in the past, so these problems may already have been addressed by recovery strategies or some of the dependent hardware resources may have recovered automatically before intervention. Reports may also be a result of valid maintenance personnel actions, even if CCS operation is severely impacted

REPT:CCS-DPC indicates a problem has occurred on the signaling paths (including alternate routes) between the GSM and a far DPC. These problems may be resolved by maintenance actions locally within the 5ESS®-2000 switch office (using procedures presented in this section), but they may be caused by problems in the CCS network (beyond link sets to an APC) where resolution is beyond the capabilities of local maintenance personnel. These procedures try to exhaust the possibilities that can be resolved locally, before assuming problems are beyond the control of the 5ESS®-2000 switch office.

PROCEDURE

1. Order the CCS entity types/error types from the REPT messages, to line up with the following listing, and CONTINUE with the next step.

NOTE: Add new items to the list if REPT output messages are produced while problem clearing is in progress. Sequence through the steps to address the most severe problem or restart the process at any time,

2. If the message

REPT MD REASON=a
SM=xxx...

appears on the ROP, where **a** is any reason **other** than **PATH IN SERVICE**, it indicates the intra-SM MD link is unavailable on a GSM **xxx**, implying all ISUP trunk and TCAP activity supported by the PSU platform on that GSM has ceased.

The loss of the intra-SM MD link may be due to autonomous recovery, where the **REPT MD** message is **CRITICALLY** alarmed, and the alarmed message is repeated at 15 minute intervals, until the problem is cleared. This report is also produced if the intra-SM MD link is manually removed (original message is unalarmed, but alarmed messages will occur thereafter at 15 minute intervals to remind office personnel of the critical nature of the manual action). There are few valid reasons to manually remove the MD link.

In 5E14 and later software releases, the **REPT MD** is still produced for information only (unalarmed); also, a

message appears indicating that internal CCS message transport has been severed in the GSM (which can only be provided by the intra-SM MD link in 5E14). The additional message appearing on the ROP is

REPT CCS MESSAGE TRANSPORT CONNECTIVITY CHANGE

GSM=a OPC=b ALL CMT CONNECTIVITY LOST

TIMESTAMP: c

where a is the target GSM number, b is its corresponding primary OPC, and c is the time when connectivity was lost. This implies that all ISUP trunk and TCAP activity supported by the PSU platform on that GSM has ceased.

The original REPT CCS MESSAGE TRANSPORT CONNECTIVITY CHANGE message will be **CRITICALLY** alarmed, unless the intra-SM MD link was manually removed. Due to the critical nature of this problem, the message will be repeated every 15 minutes, always with a **CRITICAL** alarm (even if manual action caused the original loss of CMT connectivity).

Execute the procedure "Clear GSM Intra-SM MD Link Problems," Procedure 14.2.2, immediately to recover the intra-SM MD link.

3. If an APC becomes inaccessible

REPT CCS APC SM=xxx OPC=a APC=b INACCESSIBLE

will appear on the ROP, where **xxx** is the GSM number, **a** is the origination point code (OPC) of that GSM, and **b** is the adjacent point code (APC) that has become inaccessible. This message is **CRITICALLY** alarmed.

See 235-600-750, *5ESS®-2000 Switch Output Messages Manual* for details about message formats.

Determine link set (LS) candidates that are causing the inaccessible condition:

- At an RC/V terminal, enter **16.10r** to access the SIGNALING POINT CODE view in REVIEW mode.

Specify the key fields associated with the inaccessible APC identified:

POINT CODE	(identified APC number)
GSM	(identified GSM number)

All the other fields are populated with current values and the ADJACENT field should be populated with **YES**.

Record the NORMAL LINK SET or ALTERNATE LINK SETS listed on the view, and then exit RC/V.

- If any of the link sets displayed on the 16.10 view is a CLS, designated by a number is in the range 256-511, determine the constituent LSs by issuing the input message:

OP: CCS, CLS, SET=aaa, SM=xxx

on an MCC/STLWS, where **aaa** is the identified CLS on GSM **xxx**, which will provide a list of constituent LSs.

- With the mapping of the CLS (if any) to constituent LSs, all *ordinary* LSs (in the range 1-255), associated with the APC, are known. Order the list of ordinary LSs, with the *NORMAL LINK SET* (either ordinary LS, or constituent members of a CLS) *first*.
- For each identified LS, display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on an

MCC/STLWS, where **aaa** is the identified LS number and **xxx** is its GSM number.

If the APC on the 1533 page **matches** the point code reported in the REPT CCS APC message, recover individual CCSLKs using the procedure "Clear GSM Signaling Link Problems," Procedure 14.2.1. First address deactivated (DACT) or locally inhibited/blocked CCSLKs, followed by OOSF-PH CCSLK (OOS due to unavailable PH hardware) or OOS-DL CCSLK (OOS due to unavailable access hardware), because these problems have obvious resolution techniques.

Once signaling connectivity is restored to the APC, SKIP to Step 6.

4. If access to **all** APC/DPCs associated with a specific GSM is lost, a message

**REPT CCS DPC SM=xxx OPC=a DPC=
THE OFFICE IS ISOLATED**

will appear on the ROP, where **xxx** is the affected GSM and **a** is the origination point code (OPC) of that GSM. This message is *CRITICALLY* alarmed and the alarmed message is repeated at 15 minute intervals until the problem is cleared.

The severity of this message is reduced, if one/more APCs have had signaling connectivity restored by the previous step (especially, if the APC was a regional signal transfer point). Otherwise, all DPCs are potential candidates for repair, so SKIP to Step 6.

5. If one or more DPCs associated with a specific GSM become inaccessible, one of the following messages

**REPT CCS DPC SM=xxx OPC=a DPC=b
ONE DPC INACCESSIBLE**

or

**REPT CCS DPC SM=xxx OPC=a DPC=
MULTIPLE DPCS INACCESSIBLE**

will appear on the ROP, where **xxx** is the affected GSM number, **a** is the origination point code (OPC) of that GSM, and **b** is the destination point code (DPC) that has become inaccessible (not printed if multiple DPCs have become inaccessible).

It's possible that one or more of the DPCs are now accessible, if one/more APCs have had signaling connectivity restored by Step 3 (especially, if the APC was a signal transfer point). Otherwise, all DPCs are potential candidates for repair, so SKIP to Step 6.

6. Identify inaccessible destination point codes (DPCs) remaining, and the link set (LS) candidates, that are causing the inaccessible condition:

- Obtain a list of DPCs that are inaccessible, by issuing the input message:

OP:CCS,DPC,STATUS=INACC,SM=xxx

on an MCC/STLWS, where **xxx** is the identified GSM number.

- For any DPCs identified, at an RC/V terminal, enter **16.10r** to access the SIGNALING POINT CODE view in REVIEW mode.

Specify the key fields associated with the target DPC:

POINT CODE	(identified DPC number)
GSM	(associated GSM number)

All the other fields are populated with current values.

Record the NORMAL LINK SET or ALTERNATE LINK SETS listed on the view, and then exit RC/V.

- If any of the link sets displayed on the 16.10 view is a CLS, designated by a number in the range 256-511, determine the constituent LSs. Issue the input message:

OP:CCS,CLS,SET=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the identified CLS and **xxx** is its GSM number, which provides a list of constituent LSs.

- With the mapping of the CLS (if any) to constituent LSs, all *ordinary* LSs (in the range 1-255), associated with the DPC, are known.
- Display the **1532,xxx CCS LINK SET SUMMARY** page on an MCC/STLWS, where **xxx** is the associated GSM number. Look for displayed LSs with a **RED** background in the status field (indicating *all* CCSLKs in that LS are unavailable). If the unavailable LS **matches** a LS associated with the inaccessible DPC, CONTINUE this procedure.

If **no matches** are found the inaccessibility conditions are due to conditions external to the 5ESS®-2000 switch office; SEEK TECHNICAL ASSISTANCE according to local procedures.

- For each identified LS, display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on an MCC/STLWS, where **aaa** is the LS number on GSM **xxx**.

Recover individual CCSLKs identified, using the procedures "Clear GSM Signaling Link Problems," Procedure 14.2.1. First address the deactivated (DACT) or locally inhibited/blocked CCSLKs, followed by OOSF-PH (OOS due to unavailable PH hardware) or OOS-DL (OOS due to unavailable access hardware) CCSLKs because these problems have obvious resolution techniques.

Reexecute this procedure, until all DPC/LS combinations have been addressed.

7. If a CCSLK becomes unavailable, the following message:

```
REPT CCSLK LS=a-b SM=xxx OPC=c
UNAVAIL d
e
```

will appear on the ROP, where **a** is the CCSLK's parent LS, **b** is the LS member, **xxx** is the identified GSM number, **c** is the OPC of that GSM, **d** is the supplemental status information, and **e** is the reason for CCSLK failure.

These messages are accompanied by a *MAJOR* alarm, unless a manual action caused the CCSLK removal. Consult 235-600-750, 5ESS®-2000 *Switch Output Messages Manual* (REPT:CCSLK ID) for more details about supplemental status information/reasons for failure.

Recover individual CCSLKs using the procedure "Clear GSM Signaling Link Problems," Procedure 14.2.1. Don't recover manually originated removals (CCSLKs in a deactivated or locally inhibited/blocked state), if the original reason for removal is still valid.

8. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 14.1.2: Analysis Using MCC Indicators

OVERVIEW

A second strategy is to use the master control center (MCC) to track CCS-related problems. This technique is less discriminatory because the priority of repair is not as clear.

PROCEDURE

1. Call up the **1010,xxx SM SUMMARY STATUS** MCC page for a specific GSM **xxx**, and look for off-normal CCS indicators. Indicators can be off-normal due to automatic recovery action or a valid manual action.

Compare the indicator to the following list and look for matches. If matches are found, follow the instructions to obtain supplementary information, and execute the referenced procedure.

2. If the **SEE PAGE 1530** indicator is present in the upper status block on the page, display the **1530,xxx MESSAGE DELIVERY** page on an MCC/STLWS, where **xxx** is the target GSM number.

If the status of the intra-SM MD displayed is still **off-normal** (*not ACT*), proceed directly to the procedure "Clear GSM Intra-SM MD Link Problems," Procedure 14.2.2, because all ISUP trunk and TCAP activity using the PSU platform on the GSM for signaling has ceased.

In 5E14 and later software releases, the 1530 MCC page (and the corresponding indicator on the 1010 MCC page) are no longer supported. If the intra-SM MD link is used for internal CCS message transport (the only possibility in 5E14), new indicators **SEE PAGE 1540** and **SEE PAGE 1541** will appear in the upper status block on the 1010 MCC page.

If the indicator appears, display the **1540,xxx GSM CMT STATUS** page on an MCC/STLWS, where **xxx** is the target GSM number. If the status block for **NGSM xxx** (the GSM itself) is still **RED**, proceed directly to the procedure "Clear GSM Intra-SM MD Link Problems," Procedure 14.2.2.

3. If the **SEE PAGE 1532** indicator in the lower left corner indicates an off-normal condition (RED background), display the **1532,xxx CCS LINK SET SUMMARY** page on an MCC/STLWS, where **xxx** is the target GSM number. In 5E14 and later software releases, this indicator appears in the upper status block on the 1010 MCC page.

Summary status for each equipped LS is shown. There are two types of status indicators that can lead to potential repair of child CCSLKs.

- Indicators with **RED** background, indicate that **all** CCSLKs in the LS are off-normal. These LSs should be analyzed first.
- Indicators with **GREEN** background, but text other than *ACT* indicate that one or more child CCSLKs are off-normal, but at least one CCSLK is still serving the LS. These LSs should be analyzed at a lower priority.
- Indicators with **GREEN** background (with *ACT* displayed), or **CYAN** background (*GROW* displayed), indicate no further investigation of child CCSLKs is required.

For LSs identified, display the corresponding **1533,aaa,xxx LINK SET MEMBER STATUS** page on an MCC/STLWS, where **aaa** is the identified LS number and **xxx** is its GSM number.

Every CCSLK which **does not possess an ACT** status, or is **locally/remotely inhibited** or **blocked** (L and/or R in the *INH* and/or *BLK* column) is a potential candidate for repair.

Once a list of CCSLKs is determined, use the procedure "Clear GSM Signaling Link Problems," Procedure 14.2.1 , to repair the CCSLK. Manually deactivated, locally inhibited or blocked CCSLKs may be disregarded, if a valid reason still exists to keep them in this state, *unless* the LS has no available CCSLKs remaining in a LS and inaccessibility of an APC is the result.

4. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 14.1.3: Analysis Using Off-Normal Status

OVERVIEW

This strategy uses a list of off-normal CCS entities, from selected manually requested status reports. This technique is less discriminatory than the other strategies because the priority of repair is not as clear.

The status requests cited here may be reexecuted at any time and this process can be restarted at any time. Any successful repair or new recovery action can alter the condition shown in a given status request.

PROCEDURE

1. Issue the input message:

OP:STATUS,MD

on an MCC/STLWS.

If the status displayed is **not ACT** for intra-SM MD links on any GSM, proceed directly to the procedures "Clear GSM Intra-SM MD Link Problems," Procedure 14.2.2, because all ISUP trunk and TCAP activity using the PSU platform on the affected GSM for signaling ceases when its intra-SM MD link is unavailable.

2. Determine if any inaccessible DPCs exist on a specific GSM, and identify any LS candidates denying access, such that child CCSLKs can be returned to service:

- Obtain a list of DPCs that are inaccessible to a specific GSM, by issuing the input message:

OP:CCS,DPC,STATUS=INACC,SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM number.

- For any DPCs identified, at an RC/V terminal, enter **16.10r** to access the SIGNALING POINT CODE view in REVIEW mode.

Specify the key fields associated with the DPC identified:

POINT CODE	(identified 9-digit DPC number)
GSM	(target GSM number)

All the other fields are populated with current values.

Record the NORMAL LINK SET or ALTERNATE LINK SETS listed on the view, and then exit RC/V.

- If any of the link sets displayed on the 16.10 view is a CLS, designated by a number in the range 256-511, obtain a list of the constituent LSs. Issue the input message:

OP:CCS,CLS,SET=aaa,SM=xxx

on an MCC/STLWS, where **aaa** is the identified CLS and **xxx** is its GSM number.

- With the mapping of the CLS (if any) to constituent LSs, all *ordinary* LSs (in the range 1-255), associated with the DPC, are known.
- Display the **1532,xxx CCS LINK SET SUMMARY** page on an MCC/STLWS, where **xxx** is the target GSM number.

If any displayed LS with a **RED** background in the status field (indicating all CCSLKs in the LS are unavailable) **matches** a LS associated with the inaccessible DPC, CONTINUE this procedure.

If **no matches** are found, the inaccessibility conditions are due to conditions external to the 5ESS®-2000 switch office; SEEK TECHNICAL ASSISTANCE according to local procedures.

- For each identified LS, display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on an MCC/STLWS, where **aaa** is the LS number and **xxx** is its GSM number.

Recover individual CCSLKs using the procedure "Clear GSM Signaling Link Problems," Procedure 14.2.1. First address the DACT or locally inhibited/blocked CCSLKs, followed by OOSF-PH (OOS due to unavailable PH hardware) or OOS-DL (OOS due to unavailable access hardware) CCSLKs, as these problems provide obvious resolution techniques.

Reexecute this procedure, until all DPC/LS combinations have been addressed.

3. To determine remaining unavailable CCSLKs issue the input message:

OP : CCS , GSM

on an MCC/STLWS.

Create a list of GSMs with non-ACT CCSLKs. These GSMs have a **CCS SUMMARY LINK STATUS** in the output noted as *SOME LINKS IN OFFNORMAL STATE* prior to the 5E14 software release. In 5E14 and later software releases, the output format of the **OP : CCS , GSM** is expanded, and target GSMs are identified by PARTIAL LOSS or TOTAL LOSS entries in the LINK STATUS field.

For each GSM identified, issue the command:

OP : STATUS , CCSLK , STATE=UNAV , SM=xxx

on an MCC/STLWS, where **xxx** is the target GSM.

For each CCSLK identified in the output, use the procedure "Clear GSM Signaling Link Problems," Procedure 14.2.1, to recover them.

4. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 14.2: PROBLEM CLEARING PROCEDURES

OVERVIEW

The procedures described in this section can be used to clear CCS-related problems on a GSM's PSU platform, after one of the "Problem Analysis Strategies," Procedure 14.1, has been completed, which will identify the problem with the greatest severity first.

Specifically, the following procedures are provided:

- See "Clear GSM Signaling Link Problems," Procedure 14.2.1, to clear CCS signaling link (CCSLK) problems.
- See "Clear GSM Intra-SM MD Link Problems," Procedure 14.2.2, to clear intra-SM message delivery (MD) link problems.
- See "Clear Protocol Handler Problems," Procedure 14.2.3, to clear problems in protocol handler version 3 (PH3) circuits.
- See "Clear Packet Switch Unit Common Controller Problems," Procedure 14.2.4, to clear problems in the packet switch unit common (PSUCOM) circuits.
- See "Clear DFI Signaling Data Link Access Problems," Procedure 14.2.5, to clear problems in signaling data link (SDL) access on digital facility interface (DFI) unit hardware/facilities.
- See "Clear DNU-S Signaling Data Link Access Problems," Procedure 14.2.6, to clear problems in SDL access on digital networking unit - SONET (DNU-S) hardware/facilities.

While these procedures are being used to clear CCS-related problems, other personnel may be addressing hardware/transmission faults independently and successful repair could positively impact CCS operation. Automatic recovery may also return resources for CCS use. Finally, the recovery of one CCSLK may involve the repair of hardware/facilities, which will recover other CCSLKs as a byproduct. The net result is that problems identified during analysis procedures could be resolved by an "outside source."

This "outside" resolution could result in trouble clearing procedures that seemingly terminate prematurely. These events are normal, and appropriate checks are always provided in the following procedures, to exit as soon as possible, whenever the targeted problem is resolved.

The problem clearing procedures in this section are:

PROCEDURE

1. Procedure 14.2.1 - Clear GSM Signaling Link Problems
2. Procedure 14.2.2 - Clear GSM Intra-SM MD Link Problems
3. Procedure 14.2.3 - Clear Protocol Handler Problems
4. Procedure 14.2.4 - Clear Packet Switch Unit Common Controller Problems
5. Procedure 14.2.5 - Clear DFI Signaling Data Link Access Problems
6. Procedure 14.2.6 - Clear DNU-S Signaling Data Link Access Problems

Procedure 14.2.1: Clear GSM Signaling Link Problems

OVERVIEW

This procedure resolves CCSLK problems on a specific GSM. The procedure contains appropriate instructions, if the CCSLK outages are due to PH hardware or SDL failures.

Prior to entering this procedure, identify the **specific** unavailable CCSLK targeted for recovery.

PROCEDURE

1. Display the **1533,aaa,xxx CCS LINK SET MEMBER STATUS** page on an MCC/STLWS, where **aaa** is the LS number associated with the target CCSLK and **xxx** is its GSM number.

This MCC page is referenced throughout this procedure to note status changes, to determine the location of the parent PSU channel group or DFI/DNU-S access hardware, and to use menu commands.

2. Determine the status of the target CCSLK from the 1533 MCC page, and compare with the following list:

- If **ACT**, CONTINUE with Step 3.
- If **ACT** but **locally inhibited** (*L* in the *INH* column), SKIP to Step 4.
- If **ACT** but **locally blocked** (*L* in *BLK* column), SKIP to Step 5.
- If **DACT**, SKIP to Step 6.
- If **OOSF-PH**, SKIP to Step 7.
- If **OOS-DL**, SKIP to Step 8.
- If **LKER-L1**, SKIP to Step 9.
- If **LKER-L2**, SKIP to Step 10.
- If **LKER-L3**, SKIP to Step 13.
- If **RSRC**, SKIP to Step 14.
- If **ACT** but **remotely inhibited** (*R* in *INH* column), SKIP to Step 16.
- If **ACT** but **remotely blocked** (*R* in *BLK* column), SKIP to Step 17.
- If **CONG1**, SKIP to Step 18.
- If **CONG2**, SKIP to Step 18.
- If **CONG3**, SKIP to Step 18.
- If **INIT**, SKIP to Step 19.
- If **OOST**, SKIP to Step 20.

3. The CCSLK is active (ACT), or operating normally, this procedure is not appropriate, or trouble clearing

actions have been successful; RETURN to the calling procedure.

4. The CCSLK is **locally inhibited**, and it can be uninhibited unless there is an ongoing maintenance investigation of the link that requires its continued inhibition.

Use the menu selection **7XX** on the **1533** page, or use the input message:

RST:CCSLK,SET=aaa,MEMBER=XX,STATE=INH,SM=xxx

on an MCC/STLWS, where **aaa** is the LS number, **xx** is the member number of the target CCSLK, and **xxx** is the associated GSM number, to uninhibit the link. RETURN to Step 2 to evaluate the result of this action.

5. The CCSLK is **locally blocked**, and can be unblocked unless there is an ongoing maintenance investigation of the link.

Use the menu selection **72XX** on the **1533** page, or use the input message:

RST:CCSLK,SET=aaa,MEMBER=XX,STATE=BLK,SM=xxx

on an MCC/STLWS, where **aaa** is the LS number, **xx** is the member number of the target CCSLK, and **xxx** is its GSM number, to unblock the link. RETURN to Step 2 to evaluate the result of this action.

6. The CCSLK is manually deactivated (removed) and it can be activated, unless there is an ongoing maintenance investigation. Use the menu selection **3XX** on the **1533** page, or use the input message:

RST:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,SM=xxx

on an MCC/STLWS, where **aaa** is the LS number, **xx** is the member number of the target CCSLK, and **xxx** is its GSM number, to activate the link. RETURN to Step 2 to evaluate the result of this action.

7. The CCSLK is unavailable due to "family-of-equipment" failures in parent PH hardware. Determine the **PSU shelf** and **channel group** numbers of the CCSLK from the **1533** page.

EXIT this procedure now and execute the PH hardware recovery procedure "Clear Protocol Handler Problems," Procedure 14.2.3. After hardware is restored, REENTER this procedure at Step 1, to evaluate the effects of that effort.

8. The CCSLK is unavailable due to "family-of-equipment" failures in parent access hardware/facilities. Determine the equipment number (**EN**) of the CCSLK access from the **1533** page.

— If a **DFI access is identified** (*EN begins with a D*), record the DEN, and EXIT this procedure now and execute the hardware recovery procedure "Clear DFI Signaling Data Link Access Problems," Procedure 14.2.5.

— If a **DNU-S access is identified** (*EN begins with a N*), record the NEN, and EXIT this procedure now and execute the hardware recovery procedure "Clear DNU-S Signaling Data Link Access Problems," Procedure 14.2.6.

After the associated hardware/facility is recovered, REENTER this procedure at Step 1, to evaluate the effects of that effort.

9. This CCSLK has failed to set up a nailed-up path between its PH termination and DFI/DNU-S access and periodic retries should ultimately restore the CCSLK. This should only occur due to a TSI network timeslot exhaustion in a SM (not SM-2000), or due to ODD corruption (resulting in over-engineering of the PIDB timeslots).

To monitor the attempted restoration, with maintenance personnel control, a deactivation/activation sequence may be initiated. Use the menu selection sequence **2XX,UCL**, followed by **3XX** on the **1533** page, or use the input message sequence:

```
RMV:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,UCL,SM=xxx
RST:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,SM=xxx
```

on an MCC/STLWS, where **aaa** is the LS number, **XX** is the member number of the target CCSLK, and **xxx** is its GSM number.

- If the CCSLK transitions to another state, RETURN to Step 2 to evaluate the transition.
- If the CCSLK does not transition to another state (despite retries), EXIT this procedure and SEEK TECHNICAL ASSISTANCE according to local procedures.

Continual failure may be due to over-engineering of line/trunk/features in the GSM, and will probably manifest itself with SM overload conditions. Otherwise, ODD corruption is the most likely candidate.

10. This CCSLK has failed level 2 alignment during a restoration attempt (or has lost alignment autonomously) and it is necessary to determine the underlying reason for the alignment failure.

Locate the **REPT CCSLK** message for the link on the ROP, and match the reason for removal with the following list:

- If the reason is **REMOTE OUT OF SERVICE**, EXIT this procedure and contact the remote office to isolate the problem (the remote office is sending an SIOS LSSU, which is inhibiting the CCSLK from establishing level 2).
- If the reason is **PH INITIALIZATION**, CONTINUE with Step 11 to check hardware check status.
- For any other reason, SKIP to Step 12.

11. Determine if hardware checks are inhibited for the target ACT CCS PH3, by issuing the input message:

```
OP:OFFNORM,SM=xxx
```

on an MCC/STLWS, where **xxx** is the target GSM number.

- If hardware checks are inhibited, but can be allowed for the ACT PH3, issue the input message:

```
ALW:HDWCHK,PSUPH=xxx-0-a-b
```

on an MCC/STLWS, where **xxx** is the GSM number, **a** is the PSU shelf number, and **b** is the PH number that serves the target CCSLK. Then, RETURN to Step 2 to evaluate the result of this action.

- If the decision is made to leave ACT PH3 hardware checks inhibited, or hardware checks were already allowed, CONTINUE with Step 12.

12. Periodic retries should ultimately restore the CCSLK from other level 2 failures (probably due to corrupted status/profile/routing data in the PH3) or errors on external transmission facilities, or problems at the far end APC.

To monitor the attempted restoration under maintenance personnel control, a deactivation/activation sequence may be initiated. Specifically, use the menu selection sequence **2XX,UCL** followed by **3XX** on the

1533 page, or use the input message sequence:

```
RMV:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,UCL,SM=xxx
RST:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,SM=xxx
```

on an MCC/STLWS, where **aaa** is the LS number, **xx** is the member number of the target CCSLK, and **xxx** is its GSM number.

- If the CCSLK transitions to another state, RETURN to Step 2 to evaluate the transition.
- If the CCSLK does not transition to another state (despite retries), EXIT this procedure and SEEK TECHNICAL ASSISTANCE according to local procedures.

If a **REPT** CCSLK report has a failure reason *EXCESS ERROR RATE AERM*, an excessive error rate has been detected by the alignment error rate monitor, possibly reflecting marginal quality of the transmission medium. Determine the equipment number (EN) of the CCSLK access from the **1533** page, which identifies the DFI/DNU-S facility to be investigated by transmission specialists.

13. This CCSLK has failed a level 3 link test either as an integral part of a restoration, or due to a manually initiated test. Periodic retries may ultimately restore the CCSLK.

To monitor the attempted restoration under maintenance personnel control, a deactivation/activation sequence may be initiated. Specifically, use the menu selection sequence **2XX,UCL** followed by **3XX** on the **1533** page, or use the input messages:

```
RMV:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,UCL,SM=xxx
RST:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,SM=xxx
```

on an MCC/STLWS, where **aaa** is the LS number, **xx** is the member number of the target CCSLK, and **xxx** is its GSM number.

- If the CCSLK transitions to another state, RETURN to Step 2 to evaluate the transition.
- If the CCSLK does not transition to another state (despite retries), EXIT this procedure and SEEK TECHNICAL ASSISTANCE according to local procedures.

The level 3 test is highly dependent upon local ODD data, which must be synchronized with the remote office (specifically the OPC, DPC and SLC data). Correlation should be verified by ODD engineers, and ASSERTS may be produced, which will identify ODD relations of interest.

It is also possible that facility wiring may be misconnected, allowing a valid level 2 connection, but causing level 3 data mismatches. Determine the equipment number (EN) of the CCSLK access from the **1533** page, which will identify the DFI/DNU-S facility to be investigated by a transmission specialist.

14. This CCSLK has failed due to an internal resource problem within the GSM (it is usually due to ODD errors or overload conditions). Periodic retries should ultimately restore the CCSLK.

To monitor the attempted restoration under maintenance personnel control, a deactivation/activation sequence may be initiated. Specifically, use the menu selection sequence **2XX,UCL** followed by **3XX** on the **1533** page, or use the input message sequence:

```
RMV:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,UCL,SM=xxx
RST:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,SM=xxx
```

on an MCC/STLWS, where **aaa** is the LS number, **xx** is the member number of the target CCSLK, and **xxx** is its GSM number.

- If the CCSLK transitions to another state, RETURN to Step 2 to evaluate the transition.
- If the CCSLK does not transition to another (despite retries), EXIT this procedure and SEEK TECHNICAL ASSISTANCE according to local procedures.

Resource problems may also be due to over-engineering of line/trunk/features, and will probably be manifest with overload conditions. If data access primitives fail (the ASSERT produced indicates the affected data relation), ODD engineers should be consulted. It is possible that SMP/PH3 communication is unreliable, and the PH is not being removed by fault recovery due to inhibited hardware checks. CONTINUE with Step 15 to analyze hardware check status.

15. Determine if hardware checks are inhibited for the target ACT CCS PH3, by issuing the input message:

OP: OFFNORM, SM=xxx,

on an MCC/STLWS where **xxx** is the target GSM number.

- If hardware checks are inhibited but can be allowed for the ACT PH3, issue the input message:

ALW: HDWCHK, PSUPH=xxx-0-a-b

on an MCC/STLWS, where **xxx** is the GSM number, **a** is the PSU shelf number, and **b** is the PH number that serves the target CCSLK. Then, RETURN to Step 2 to evaluate the result of this action.

- If the decision is made to leave ACT PH3 hardware checks inhibited, or hardware checks were already allowed, SEEK TECHNICAL ASSISTANCE according to local procedures.

16. The CCSLK is **remotely inhibited**. The only recourse is to notify the far-end exchange to uninhibit the link. The far-end APC is identified on the **1533** page.

- If cooperation is achieved, RETURN to Step 2 to evaluate the effects of this action.
- If the far-end exchange will not uninhibit the CCSLK, no further action is possible locally; RETURN to the calling procedure.

17. The CCSLK is **remotely blocked**. The only recourse is to notify the far-end exchange to unblock the link. The APC is identified on the **1533** page.

- If cooperation is achieved, RETURN to Step 2 to evaluate the effects of this action.
- If the far-end exchange will not unblock the CCSLK, no further action is possible locally; RETURN to the calling procedure.

18. This CCSLK is active (ACT), but some level of congestion throttles are in effect, restricting traffic flow. This situation should be self-correcting with the automatic application/relaxation of throttles in burst traffic situations. If the condition is persistent (excessive entries into various levels of congestion during busy hour), problems may be resolved by reprovisioning, specifically:

- If one/more CCSLK in the same LS are unavailable, congestion throttles may be expected; repair the other links in the LS, before carrying out a provisioning investigation.

- Check various congestion threshold values in office records and adjust them using the procedure "Modify Link Member Characteristics," Procedure 13.1.14 .
- Congestion may be caused by improper engineering of PH3/LS resources. Check office records to determine if too many links are assigned to a given channel group, or too few CCSLKs are provisioned in a given LS. If new CCSLKs are to be assigned, or channel group reassignment is required, see the provisioning procedure "Define New Link Set Members," Procedure 13.1.10 , or "Modify Link Member Characteristics," Procedure 13.1.14 , respectively.

In any event, EXIT this procedure.

19. The CCSLK is initializing, and should make a state transition shortly. Allow the restoration attempt to complete, and then RETURN to Step 2 to evaluate the results of this action.

To monitor the attempted restoration under maintenance personnel control, a deactivation/activation sequence may be initiated. Specifically, use the menu selection sequence **2XX,UCL** followed by **3XX** on the **1533** page, or use the input message:

```
RMV:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,UCL,SM=xxx
RST:CCSLK,SET=aaa,MEMBER=XX,STATE=DACT,SM=xxx
```

on an MCC/STLWS, where **aaa** is the LS number, **xx** is the member number of the target CCSLK, and **xxx** its GSM number.

- If the CCSLK transitions to another state, RETURN to Step 2 to evaluate the transition.
 - If the CCSLK does not transition to another state (despite retries), EXIT this procedure and SEEK TECHNICAL ASSISTANCE according to local procedures.
20. The CCSLK is changing state (transient condition) due to actions of a maintenance process. Allow the maintenance activity to complete, and then RETURN to Step 2 to evaluate the results of this action.
 21. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 14.2.2: Clear GSM Intra-SM MD Link Problems

OVERVIEW

This procedure resolves problems identified for the intra-SM MD link on a specific GSM. The procedure contains appropriate instructions if MD link outage is due to PH hardware failures.

PROCEDURE

1. On the MCC/STLWS, issue the input message

OP : STATUS , MD , SM=xxx

where xxx is the target GSM.

2. Determine the status of the target intra-SM MD link from the output produced, and compare with the following list:
 - If ACTIVE, CONTINUE with Step 3.
 - If OOS-DEACTIVATED, SKIP to Step 4.
 - If OOS-FAMILY PH, SKIP to Step 5.
 - If OOS-LINK ERROR, SKIP to Step 6.
 - If INITIALIZING, SKIP to Step 6.
 - If OOS-TRANSIENT, allow the state to stabilize, and then return to Step 1.

3. The intra-SM MD link is ACTIVE, or operating normally, this procedure is not appropriate, or trouble clearing actions have been successful; RETURN to the calling procedure.
4. The intra-SM MD link is manually deactivated (removed), and should be restored. Use the input message:

RST : MD , SM=xxx

where **xxx** is the associated GSM number, to activate the link. RETURN to Step 1 to evaluate the result of this action.

5. The intra-SM MD is unavailable due to "family-of-equipment" failures in parent PH hardware. Determine the **PSU shelf** and **channel group** numbers of the MD link from the OP STATUS MD output in Step 1.

EXIT this procedure now and execute the PH hardware recovery procedure "Clear Protocol Handler Problems," Procedure 14.2.3 for the identified channel group. After hardware is repaired and/or restored, REENTER this procedure at Step 1 to evaluate the effects of that effort.

6. The intra-SM MD link is awaiting restoration and should make a state transition shortly (or restoration retries are scheduled automatically). Allow the restoration attempt to complete, and RETURN to Step 1 to evaluate the results of this action.

To monitor the attempted restoration under maintenance personnel control, a deactivation/activation sequence may be initiated. Specifically, use the input message sequence:

RMV:MD,SM=xxx,UCL
RST:MD,SM=xxx

on an MCC/STLWS, where **xxx** is the associated GSM number.

- If the MD link transitions to another state (the status is reported via an autonomous REPT MD message), RETURN to Step 2 to evaluate the transition.
- If the MD link does not transition to another state (despite retries), EXIT this procedure and SEEK TECHNICAL ASSISTANCE according to local procedures.

7. STOP. YOU HAVE COMPLETED THIS PROCEDURE.

Procedure 14.2.3: Clear Protocol Handler Problems

OVERVIEW

This procedure resolves problems in the protocol handler version 3 (PH3) or version 22 (PH22) units on PSU shelves, that support CCSLK or intra-SM MD link functionality (that is, MD, ST7, or MDST7 channel group types). The procedure is **not** intended as a general PH repair procedure.

Determine the PSUCOM shelf to repair before entering this procedure.

PROCEDURE

1. Display the **118y,xxx PSU 0 SHELF y** page on an MCC/STLWS, where **y** is the target PSU shelf in the range 0-4 on a GSM **xxx**.

Observe the status of all **PH3s**, and the **CHANNEL GROUP SUMMARY** (looking for CCS channel groups of type MD, MDST7, or ST7).

- If there are one/more unassigned CCS channel groups (indicator on the right side of the MCC page will have a RED background), choose an **OOS PH3** to repair and CONTINUE this procedure.
- Otherwise, RETURN to the calling procedure, because it is not appropriate to resolve CCS problems in the PSU complex.

In 5E14 and later software releases, CCS channel groups can be provisioned on **PH22s** as well as PH3s. When interrogating unassigned CCS channel groups, it is important to note the *PH hardware type* supporting the identified channel group, and the appropriate OOS PH3 or PH22 must be analyzed by the remainder of this procedure.

2. If the status of **all** equipped PHs is **OOSF** (OOS for "family-of-equipment" reasons), an ACT PSUCOM does not exist. EXIT this procedure immediately, and execute the procedure "Clear Packet Switch Unit Common Controller Problems," Procedure 14.2.4, to resolve the duplex failed PSUCOM situation.
3. For the OOS PH3 or PH22 chosen, determine detailed status by issuing the input message:

OP:CFGSTAT,SM=xxx,OOS,NOFE

where **xxx** is the target GSM number.

- If the state is **OOS-MAN-RMV**, SKIP to Step 4.
- If the state is **OOS-AUTO-RMV**, SKIP to Step 6.
- If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 7.
- If the state is **OOS-MAN-EX**, SKIP to Step 7.
- If the state is **OOS-REX-RMV**, SKIP to Step 8.
- If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 9.
- If the state is **OOS-AUTO-TBLA**, SKIP to Step 10.

4. Restore the PH3 or PH22 by using the menu selection **3XX** on the 118y MCC page, or the input message:

RST : PSUPH=xxx-0-a-XX

where **xxx** is the target GSM number, **a** is the PSUCOM shelf number, and **xx** is the physical PH number.

5. Did the PH3 or PH22 restore successfully to ACT?

— If **yes**, RETURN to Step 1.

— If **no**, RETURN to Step 2.

6. The PH3 or PH22 has been automatically removed for the purpose of running diagnostics. Allow the diagnostic to be scheduled because a problem has been detected by fault recovery. After the diagnostic completes, RETURN to Step 1.
7. The PH3 or PH22 is currently being diagnosed or manually exercised. When the diagnostics completes, or an interactive exercise session is stopped, RETURN to Step 1.
8. The PH3 or PH22 is currently being routinely exercised. Since PH channel groups are unassigned, the routine exercise should be stopped immediately. Use the input message:

STP : PSUPH=xxx-0-a-XX

on an MCC/STLWS, where **xxx** is the target GSM number, **a** is the PSUCOM shelf number, and **xx** is the physical PH number. Then RETURN to Step 1 for re-evaluation.

9. The PH3 or PH22 is faulty. Find the most recent printed trouble location procedure (TLP) list on the ROP, and use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS[®]-2000 Switch" in the 235-105-220 , *5ESS[®]-2000 Switch Corrective Maintenance Procedures Manual*. After the repair is completed, including the attempted restoration of the PH3 or PH22, is the PH successfully restored to ACT?

— If **yes**, RETURN to Step 1.

— If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure, for the affected PH.

If CCS channel groups on the target shelf are still unassigned, and there are other OOS PH3 or PH22 candidates that may still be successfully recovered, choose a new PH3 or PH22 and RETURN to Step 2.

10. The PH3 or PH22 is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure, for the affected PH.

11. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 14.2.4: Clear Packet Switch Unit Common Controller Problems

OVERVIEW

This procedure resolves duplex failed packet switch unit common controller (PSUCOM) circuitry outages, which affect all CCS operation on a GSM's PSU platform. This is not a general PSUCOM repair procedure.

PROCEDURE

1. Display the **1186,xxx PSU NETWORK** page on an MCC/STLWS, where **xxx** is the target GSM.

Observe the status of both PSUCOMs.

- If **both** PSUCOMs are out-of-service (OOS), indicating a duplex failure, CONTINUE with Step 2. Start with the repair of PSUCOM 0.
- Otherwise, this procedure is not appropriate to resolve CCS problems; EXIT this procedure immediately.

2. For the PSUCOM chosen, determine a detailed status by issuing the input message:

OP:CFGSTAT,SM=xxx,OOS,NOFE

on an MCC/STLWS, where **xxx** is the target GSM number.

- If the state is **OOS-MAN-RMV**, CONTINUE with Step 3.
- If the state is **OOS-AUTO-RMV**, SKIP to Step 5.
- If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 6.
- If the state is **OOS-MAN-EX**, SKIP to Step 6.
- If the state is **OOS-REX-RMV**, SKIP to Step 7.
- If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 8.
- If the state is **OOS-AUTO-TBLA**, SKIP to Step 9.

3. Restore the PSUCOM, by using the menu selection **30X** on the **1186** MCC page, or the input message:

RST:PSUCOM=xxx-0-X

at an MCC/STLWS, where **xxx** is the target GSM number, and **x** is the PSUCOM side.

4. Did the PSUCOM restore successfully?

- If **yes**, RETURN to Step 1.
- If **no**, RETURN to Step 2.

5. The PSUCOM has been automatically removed for the purpose of running diagnostics. Allow the diagnostic

to be completed because a problem has been detected by fault recovery. After the diagnostic completes, RETURN to Step 1.

6. The PSUCOM is being diagnosed.

Allow automatic diagnostics to complete, then RETURN to Step 2.

Otherwise, since this is a PSUCOM duplex failure recovery, interactive exercise/manual diagnostics should be stopped/aborted immediately, unless the diagnostic activity is part of a repair procedure. Issue the input message:

STP : PSUCOM=xxx-0-X

at an MCC/STLWS, where **xxx** is the target GSM number, and **x** is the PSUCOM side.

If this input message fails use

ABT : PSUCOM=xxx-0-X

and then RETURN to Step 2.

7. The PSUCOM is currently being routinely exercised. Since this is a PSUCOM duplex failure recovery, routine exercise should be stopped immediately, using the input message:

STP : PSUCOM=xxx-0-X

at an MCC/STLWS, where **xxx** is the target GSM number, and **x** is the PSUCOM side. Then RETURN to Step 2.

8. The PSUCOM is faulty. Find the most recent printed trouble location procedure (TLP) list on the ROP, use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS®-2000 Switch" in the 235-105-220 , *5ESS®-2000 Switch Corrective Maintenance Procedures Manual*. When the repair is completed, including the attempted restoration of the PSUCOM, is the PSUCOM successfully restored?

— If **yes**, RETURN to Step 1.

— If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure for the affected PSUCOM.

If PSUCOM 0 is currently being processed, RETURN to Step 2 to attempt the repair of PSUCOM 1, if PSUCOM 1 is still OOS.

9. The PSUCOM is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure for the affected PSUCOM.
10. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 14.2.5: Clear DFI Signaling Data Link Access Problems

OVERVIEW

This procedure resolves problems associated with a signaling data link (SDL) on a GSM, or its parent digital facilities interface (DFI) hardware and corresponding T1 facilities.

Before entering this procedure, identify the specific SDL that needs repair. Specifically, the corresponding digital equipment number (DEN) must be known; it has the form:

DEN=a-b-xx-c

where **a** is the target GSM number, **b** is the DLTU (digital line trunk unit), **xx** is the DFI number, and **c** is the DS0 channel number.

On a DFI version 2 (DFI2), the **TI facility** can be identified, by noting that a DS0 channel in the range 1-24 is on facility **0**, and a channel in the range 25-48 is on facility **1**.

PROCEDURE

1. First determine the status of the SDL port, by issuing the input message:

OP:STATUS,DEN=a-b-xx-c

on an MCC/STLWS, where **a-b-xx-c** is the specified SDL DEN in the form previously noted.

Based upon the state of the SDL, perform the following action:

- If the state is **IS**, the SDL is in-service (either initially or due to recovery action), so this procedure is not appropriate, RETURN to the calling procedure.
- If the state is **OOS-MTCE-DSBLD**, CONTINUE with Step 2.
- If the state is **OOS-MTCE-FAF**, SKIP to Step 3.
- If the state is **OOS-MTCE-FE**, SKIP to Step 3.
- For any other state, SEEK TECHNICAL ASSISTANCE according to local practices.

2. The SDL port has been manually removed (unconditionally) and the port should be restored manually. Issue the input message:

RST:TRK,DEN=a-b-xx-c,UCL

on an MCC/STLWS, where **a-b-xx-c** is the SDL DEN in the form previously noted.

After the restoration process completes, RETURN to Step 1 for reevaluation.

3. The SDL port is OOS due to parent DFI/DFI2 hardware/facility failures. Display the **112v,b,a DLTU b** page on an MCC/STLWS, where **v** is 0 for DFI numbers in the range (1,4), 1 for DFI numbers in the range (5,8) and 2 for DFI numbers in the range (9,10); **b** is the DLTU number (derived from the target DEN); and **a** is its GSM number.

Observe the status of the **DFI** and the **T1 facility**, including the type of carrier group alarm (CGA), if present, associated with the target SDL's facility (information derived from the target DEN).

Proceed according to the following discrimination:

- If the target **DFI** is **OOS**, CONTINUE with Step 4.
- If there is a **CGA** present on the target facility, SKIP to Step 11.
- If the target **T1 facility** is **OOS** (no CGA), SKIP to Step 12.
- If the target **T1 facility** is **DGR** and the SDL port status is **OOS-MAN-FE**, SKIP to Step 14.
- Otherwise, RETURN to Step 1 to re-evaluate SDL status.

4. For the OOS DFI identified, determine a detailed status by issuing the input message:

OP:CFGSTAT,SM=a,OOS,NOFE

where **a** is the target GSM number.

- If the state is **OOS-MAN-RMV**, CONTINUE with Step 5.
- If the state is **OOS-AUTO-RMV**, SKIP to Step 7.
- If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 8.
- If the state is **OOS-MAN-EX**, SKIP to Step 8.
- If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 9.
- If the state is **OOS-AUTO-TBLA**, SKIP to Step 10.

5. Restore the DFI by using the menu selection **30xx** on the 112v page, or the input message:

RST:DFI=a-b-xx

where **a** is the target GSM number, **b** is the DLTU number, and **xx** is the DFI number).

6. Did the DFI restore successfully to ACT?

- If **yes**, RETURN to Step 1 to re-evaluate SDL status.
- If **no**, RETURN to Step 3.

7. The DFI has been automatically removed for the purpose of running diagnostics. Allow the diagnostic to be completed because a problem has been detected by fault recovery. After the diagnostic completes, RETURN to Step 3.
8. The DFI is currently being diagnosed, or manually exercised. When the diagnostics completes, or an interactive exercise session is stopped, RETURN to Step 3.
9. The DFI is faulty. Find the most recent printed trouble location procedure (TLP) list on the ROP, use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS[®]-2000 Switch" in the 235-105-220,

5ESS®-2000 Switch Corrective Maintenance Procedures Manual. When the repair is completed, including the attempted restoration of the DFI, is the DFI successfully restored to ACT?

- If **yes**, RETURN to Step 1 to re-evaluate the impact on the SDL.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

10. The DFI is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure.
11. If the facility is experiencing a CGA (data from the 112v MCC page will indicate whether the alarm is local, remote or an alarm indication signal), consult experienced transmission specialists, because the problem is probably in *non-5ESS®-2000* Switch equipment. SEEK TECHNICAL ASSISTANCE according to local procedure.

Once the CGA is cleared, reenter this procedure to re-evaluate the effect on the target SDL.

12. Restore the affected OOS facility, using the menu selection **31xxz** on the 112v MCC page, or the input message:

RST : FAC=a-b-xx-z

where **a** is the target GSM number, **b** is the DLTU number, **xx** is the DFI number, and **z** is the DFI facility number.

13. Did the DFI facility restore successfully to ACT?

- If **yes**, RETURN to Step 1 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

14. The affected DFI facility is degraded (DGR), from a previous failed removal attempt. Restore the DGR facility, using the menu selection **31xxz,UCL** on the 112v MCC page, or the input message:

RST : FAC=a-b-xx-z , UCL

where **a** is the target GSM number, **b** is the DLTU number, **xx** is the DFI number, and **z** is the DFI facility number.

15. Did the DFI facility restore successfully to ACT?

- If **yes**, RETURN to Step 1 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

16. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

Procedure 14.2.6: Clear DNU-S Signaling Data Link Access Problems

OVERVIEW

This procedure resolves problems with signaling data link (SDL) ports on a GSM, or its parent digital networking unit - SONET (DNU-S) access hardware/facilities. This includes the DNU-S common control (DNUSCC), the DNU-S common data (DNUSCD), transmission multiplexer (TMUX), or STSX-1 facility interface (SFI) hardware, and various levels of SONET facilities.

Before entering this procedure, identify a specific SDL, the corresponding network equipment number (NEN) has the form in pre-5E13 software releases:

NEN=a-b-x-y-vv-c

where **a** is the target GSM number, **b** is the digital network unit - SONET (DNU-S) number, **x** is the data group (DG), **y** is the synchronous transport signal (STS) number, **vv** is the virtual tributary 1.5 (VT1.5), and **c** is the DS0 channel number in the range 1-24.

For 5E13 and later software releases, the NEN definition was altered to redefine the synchronous transport signal and virtual tributary numbering conventions to accommodate Bellcore standards, specifically:

NEN=a-b-x-s-y-g-m-c

where **a** is the target GSM number, **b** is the digital network unit-SONET (DNU-S) number, **x** is the data group (DG), **s** is the SONET termination equipment number, **y** is the synchronous transport signal number, **g** is the virtual tributary group, **m** is the virtual tributary member, and **c** is the DS0 channel number.

PROCEDURE

1. Execute procedures dependent upon the software release available in the office:
 - If prior to the 5E13 software release, CONTINUE this procedure.
 - If 5E13 or later software release, SKIP to Step 50.

2. Determine the status of the SDL, by issuing the input message:

OP: STATUS, NEN=a-b-x-y-vv-c

on an MCC/STLWS, where **a-b-x-y-vv-c** is the specified SDL NEN in the form previously noted.

Based upon the state of the SDL, perform the following action:

- If the state is **IS**, the SDL is in-service (due to recovery action, internal/external to this procedure) so this procedure is not appropriate; RETURN to the calling procedure.
- If the state is **OOS-MTCE-DSBLD**, CONTINUE with Step 3.
- If the state is **OOS-MTCE-FAF**, SKIP to Step 4.
- If the state is **OOS-MTCE-FE**, SKIP to Step 4.
- For any other state, SEEK TECHNICAL ASSISTANCE according to local practices.

3. The SDL port has been manually removed (unconditionally), and the port should be restored manually. Issue the input message:

RST:TRK,NEN=a-b-x-y-vv-c,UCL

on an MCC/STLWS, where **a-b-x-y-vv-c** is the SDL NEN in the form previously noted.

When the restoration is completed, RETURN to Step 1 for re-evaluation.

4. The SDL is OOS due to a DNU-S hardware/facility failure. Therefore, display the **1510,b,a DNUS b STATUS** page on an MCC/STLWS, where **b** is the DNU-S number (derived from the target NEN) and **a** is its GSM number.

Observe the status of DNU-S common control (**DNUSCC**), the DNUS common data (**DNUSCD**), and the STS-1 facility interface (**SFI**), where the DNUSCDs or SFIs to be investigated are associated with the data group (DG) identified in the NEN.

Proceed according to the following:

- If **both DNUSCCs** are OOS, indicating a duplex failure, CONTINUE with Step 5. Start with the repair of DNUSCC 0.
- If **both DNUSCDs** associated with data group **x** are OOS, indicating a duplex failure, SKIP to Step 13. Start with the repair of DNUSCD 0.
- If **both SFIs** associated with data group **x** are OOS, indicating a duplex failure, SKIP to Step 21. Start with the repair of SFI 0.
- Otherwise, SKIP to Step 29.

5. For the DNUSCC side **z** chosen, determine a detailed status by issuing the input message:

OP:CFGSTAT,SM=a,OOS,NOFE

where **a** is the target GSM number.

- If the state is **OOS-MAN-RMV**, CONTINUE with Step 6.
- If the state is **OOS-AUTO-RMV**, SKIP to Step 8.
- If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 9.
- If the state is **OOS-MAN-EX**, SKIP to Step 9.
- If the state is **OOS-REX-RMV**, SKIP to Step 10.
- If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 11.
- If the state is **OOS-AUTO-TBLA**, SKIP to Step 12.

6. Restore the DNUSCC, by using the menu selection **30z** on the **1510** MCC page, or the input message:

RST:DNUSCC=a-b-z

on an MCC/STLWS, where **a** is the GSM target number, **b** is the DNU-S number, and **z** is the DNUSCC side.

7. Did the DNUSCC restore successfully?

— If **yes**, RETURN to Step 2.

— If **no**, RETURN to Step 5.

8. The DNUSCC has been automatically removed for the purpose of running diagnostics. Allow the diagnostic to be scheduled because a fault has been detected by fault recovery. After the diagnostic completes, RETURN to Step 4.

9. The DNUSCC is currently being diagnosed, or manually exercised.

Allow automatic diagnostics to complete and then RETURN to Step 4.

Since this is a DNUSCC duplex failure recovery, interactive exercise/manual diagnostics should be stopped/aborted immediately, unless the diagnostic activity is part of a current repair procedure. Issue the input message:

STP:DNUSCC=a-b-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, and **z** is the DSUSCC side.

If this request fails, use

ABT:DNUSCC=a-b-z

and then RETURN to Step 4.

10. The DNUSCC is currently being routinely exercised. Since this is a DNUSCC duplex failure recovery, routine exercise should be stopped immediately, using the input message:

STP:DNUSCC=a-b-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, and **z** is the DNUSCC side. RETURN to Step 4.

11. The DNUSCC is faulty. Find the most recent printed trouble location procedure (TLP) list on the ROP. Use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS[®]-2000 Switch" in the 235-105-220, *5ESS[®]-2000 Switch Corrective Maintenance Procedures Manual*. When the repair is completed, including the attempted restoration of the DNUSCC, is the DNUSCC successfully restored?

— If **yes**, RETURN to Step 2.

— If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure for the affected DNUSCC.

If DNUSCC 0 is being processed, RETURN to Step 5 to attempt the repair of DNUSCC 1, if DNUSCC 1 is still OOS.

12. The DNUSCC is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure for the affected DNUSCC.

If DNUSCC 0 is currently being processed, RETURN to Step 5 to attempt the repair of DNUSCC 1, if DNUSCC 1 is still OOS.

13. For the DNUSCD side **z** chosen, determine a detailed status by issuing the input message:

OP:CFGSTAT,SM=a,OOS,NOFE

where **a** is the target GSM number.

- If the state is **OOS-MAN-RMV**, CONTINUE with Step 14.
- If the state is **OOS-AUTO-RMV**, SKIP to Step 16.
- If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 17.
- If the state is **OOS-MAN-EX**, SKIP to Step 17.
- If the state is **OOS-REX-RMV**, SKIP to Step 18.
- If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 19.
- If the state is **OOS-AUTO-TBLA**, SKIP to Step 20.

14. Restore the DNUSCD, by using the menu selection **31xz** on the 1510 MCC page, or the input message:

RST:DNUSCD=a-b-x-z

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the DNUSCD side.

15. Did the DNUSCD restore successfully?

- If **yes**, RETURN to Step 2 to re-evaluate SDL status.
- If **no**, RETURN to Step 13.

16. The DNUSCD has been automatically removed for the purpose of running diagnostics. Allow the diagnostic to be scheduled, because a fault has been detected by fault recovery. After the diagnostic completes, RETURN to Step 2.

17. The DNUSCD is currently being diagnosed, or manually exercised.

Allow automatic diagnostics to complete and then RETURN to Step 4.

Since this is a DNUSCD duplex failure recovery, interactive exercise/manual diagnostics should be stopped/aborted immediately, unless the diagnostic activity is part of a current repair procedure. Issue the input message:

STP:DNUSCD=a-b-x-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the DSUSCD side.

If this request fails, use

ABT:DNUSCD=a-b-x-z

and then RETURN to Step 13.

18. The DNUSCD is currently being routinely exercised. Since this is a DNUSCD duplex failure recovery, routine exercise should be stopped immediately, using the input message:

STP:DNUSCD=a-b-x-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the DSUSCD side.

If this request fails, use

ABT:DNUSCD=a-b-x-z

then RETURN to Step 2.

19. The DNUSCD is faulty. Find the most recent printed trouble location procedure (TLP) list on the ROP. Use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS®-2000 Switch" in the 235-105-220, *5ESS®-2000 Switch Corrective Maintenance Procedures Manual*. When the repair is completed, including the attempted restoration of the DNUSCD, is the DNUSCD successfully restored?
- If **yes**, RETURN to Step 2 to re-evaluate SDL status.
 - If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure for the affected DNUSCD.
- If DNUSCD 0 is being processed, RETURN to Step 13 to attempt the repair of DNUSCD 1, if DNUSCD 1 is still OOS.
20. The DNUSCD is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure, but if DNUSCD 0 is currently being processed, RETURN to Step 13 to attempt the repair of DNUSCD 1, if DNUSCD 1 is still OOS.
21. For the SFI side **z** chosen, determine a detailed status by issuing the input message:
- OP:CFGSTAT,SM=a,OOS,NOFE**
- where **a** is the target GSM number.
- If the state is **OOS-MAN-RMV**, CONTINUE with Step 22.
 - If the state is **OOS-AUTO-RMV**, SKIP to Step 24.
 - If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 25.
 - If the state is **OOS-MAN-EX**, SKIP to Step 25.
 - If the state is **OOS-REX-RMV**, SKIP to Step 26.
 - If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 27.
 - If the state is **OOS-AUTO-TBLA**, SKIP to Step 28.
22. Restore the SFI, by using the menu selection **32xz** on the 1510 MCC page, or the input message:

RST:SFI=a-b-x-z

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the SFI side.

23. Did the SFI restore successfully?

- If **yes**, RETURN to Step 2 to re-evaluate SDL status.
- If **no**, RETURN to Step 21.

24. The SFI has been automatically removed for the purpose of running diagnostics. Allow the diagnostic to be scheduled because a fault has been detected by fault recovery. After the diagnostic completes, RETURN to Step 2.

25. The SFI is currently being diagnosed, or manually exercised.

Allow automatic diagnostics to complete and then RETURN to Step 21.

Since this is a SFI duplex failure recovery, interactive exercise/manual diagnostics should be stopped/aborted immediately, unless the diagnostic activity is part of a current repair procedure. Issue the input message:

STP:SFI=a-b-x-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the SFI side.

If this request fails, use

ABT:SFI=a-b-x-z

and then RETURN to Step 13.

26. The SFI is currently being routinely exercised. Since this is an SFI duplex failure recovery, routine exercise should be stopped immediately, using the input message:

STP:SFI=a-b-x-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the SFI side.

If this request fails, use

ABT:SFI=a-b-x-z

and then RETURN to Step 2.

27. The SFI is faulty. Find the most recent printed TLP list on the ROP. Use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS[®]-2000 Switch" in the 235-105-220, *5ESS[®]-2000 Switch Corrective Maintenance Procedures Manual*. When the repair is completed, including the attempted restoration of the SFI, is the SFI successfully restored?

- If **yes**, RETURN to Step 2 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure for the affected SFI.

If SFI 0 is being processed, RETURN to Step 21 to attempt the repair of SFI 1 (if SFI 1 is still OOS).

28. The SFI is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure for the affected SFI.

If SFI 0 is currently being processed, RETURN to Step 21 to attempt the repair of SFI 1 (if SFI 1 is still OOS).

29. Display the **1510,b,a DNUS b STATUS** page on an MCC/STLWS, where **b** is the DNU-S number (from the target NEN) and **a** is its GSM number.

Observe the status of the **TMUX**, and SONET terminating equipment (**STE**) facility, including the type of carrier group alarm (**CGA**) associated with the **STS** number **y** in the NEN, and data group **x**. Also, note the status of the **spare TMUX** (the last TMUX in the target DG).

Proceed according to the following:

- If **TMUX** serving the target STE facility is **OOS**, SKIP to Step 30.
- If there is a **CGA** present on the target STE facility, SKIP to Step 37.
- If the affected **STE** is OOS (no CGA and parent TMUX is ACT), SKIP to Step 38.
- Otherwise, SKIP to Step 40.

30. For the OOS TMUX **y** in data group **x** chosen, determine a detailed status by issuing the input message:

OP:CFGSTAT,SM=a,OOS,NOFE

where **a** is the target GSM number.

- If the state is **OOS-MAN-RMV**, SKIP to Step 31.
- If the state is **OOS-AUTO-RMV**, SKIP to Step 33.
- If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 34.
- If the state is **OOS-MAN-EX**, SKIP to Step 34.
- If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 35.
- If the state is **OOS-AUTO-TBLA**, SKIP to Step 36.

31. Restore the TMUX, by using the menu selection **33xy** on the 1510 MCC page, or the input message:

RST:TMUX=a-b-x-y

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **y** is the TMUX number (corresponding to the STS number in the target NEN).

32. Did the TMUX restore successfully to ACT?

- If **yes**, RETURN to Step 2 to re-evaluate SDL status.
- If **no**, RETURN to Step 30.

33. The TMUX has been automatically removed for the purpose of running diagnostics. Allow the diagnostic to be scheduled because a fault has been detected by fault recovery. When the diagnostic completes, RETURN to Step 2.
34. The TMUX is currently being diagnosed, or manually exercised. When the diagnostic completes, or an interactive exercise session is stopped, RETURN to Step 2.
35. The TMUX is faulty. Find the most recent printed TLP list on the ROP. Use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS®-2000 Switch" in the 235-105-220, *5ESS®-2000 Switch Corrective Maintenance Procedures Manual*. When the repair is complete, including the attempted restoration of the TMUX, is the TMUX successfully restored to ACT?

— If **yes**, RETURN to Step 2 to re-evaluate the impact on the SDL.

— If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure for the affected TMUX.

If the **spare TMUX** is OOS, RETURN to Step 30 to attempt recovery of that unit.

36. The TMUX is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure for the affected TMUX, but if the **spare TMUX** is OOS, RETURN to Step 30 to attempt recovery of that unit.
37. If the STE facility is experiencing a CGA (data from the 1510 MCC page indicates whether the alarm is local, remote, or an alarm indication signal), consult experienced transmission specialists, because the problem is probably in non-SM equipment. SEEK TECHNICAL ASSISTANCE according to local procedure.

Once the CGA is cleared, reenter this procedure to re-evaluate the effect on the target SDL.

38. Restore the affected OOS STE facility, using the menu selection **34xy** on the 1510 MCC page, or the input message:

RST:STEFAC=a-b-x-y

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **y** is the STE facility number (corresponding to the STS number in the target NEN).

39. Did the STE facility restore successfully to ACT?
 - If **yes**, RETURN to Step 2 to re-evaluate SDL status.
 - If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.
40. From the 1510 page, display the **1511,b,y DNUS b FAC y** page on an MCC/STLWS, where **b** is the DNU-S number, and **y** is the synchronous transport signal - level 1 (STS-1) facility number, from the target NEN.

Check the status of the **STS-1**, **VT1.5** and **DS1** facilities, associated with the **VT1.5** number in the NEN, including the type of VT1.5 carrier group alarm (CGA).

Proceed according to the following:

— If the affected **STS-1 facility** is OOS, SKIP to Step 41.

— If there is a **CGA** present on the target VT1.5 facility, SKIP to Step 43.

- If the affected **VT1.5 facility** is OOS (not OOSF and no CGA), SKIP to Step 44.
- If the affected **DS1 facility** is OOS (not OOSF), SKIP to Step 46.
- If the affected **DS1 facility** is **DGR** and the SDL status is **OOS-MAN-FE**, SKIP to Step 48.
- If none of the above, RETURN to Step 2 to re-evaluate SDL status.

41. Restore the affected OOS STS-1 facility, using the menu selection **3000** on the *1511* MCC page, or the input message:

RST:STS1FAC=a-b-x-y

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **y** is the STS-1 number.

42. Did the STS-1 facility restore successfully to ACT?

- If **yes**, RETURN to Step 2 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

43. If the VT1.5 facility is experiencing a CGA (data from the *1511* MCC page indicates whether the alarm is local, remote or an alarm indication signal), consult experienced transmission specialists, because the problem is probably in non-SM equipment. SEEK TECHNICAL ASSISTANCE according to local procedure.

Once the CGA is cleared, reenter this procedure to re-evaluate the effect on the target SDL.

44. Restore the affected OOS VT1.5 facility, using the menu selection **31vv** on the *1511* MCC page (where **vv** must be expressed in two-digit format), or the input message:

RST:VT1FAC=a-b-x-y-vv

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, **y** is the STS-1 number, and **vv** is the VT1.5 facility number.

45. Did the VT1.5 facility restore successfully to ACT?

- If **yes**, RETURN to Step 2 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

46. Restore the affected OOS DS1 facility using the menu selection **32vv** on the *1511* MCC page (where **vv** must be expressed in two-digit format), or the input message:

RST:DS1SFAC=a-b-x-y-vv

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, **y** is the STS-1 number, and **vv** is the parent VT1.5 facility number.

47. Did the DS1 facility restore successfully to ACT?

- If **yes**, RETURN to Step 2 to re-evaluate SDL status.

— If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

48. The affected DS1 facility is degraded (DGR) from a previous failed removal attempt. Therefore, restore the degraded facility using the menu selection **32vv,UCL** on the 1511 MCC page (where **vv** must be expressed in two-digit format), or the input message:

RST:DS1SFAC=a-b-x-y-vv,UCL

where **a** is the GSM number, **b** is the DNU-S number, **x** is the DG number, **y** is the STS-1 number, and **vv** is the parent VT1.5 facility number.

49. Did the DS1 facility restore successfully to ACT?

— If **yes**, RETURN to Step 2 to re-evaluate SDL status.

— If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

50. Determine the status of the SDL by issuing the input message:

OP:STATUS,NEN=a-b-x-s-y-g-m-c

on an MCC/STLWS, where **a-b-x-s-y-g-m-c** is the specified SDL NEN in the form previously noted.

Based upon the state of the SDL, perform the following action:

- If the state is **IS**, the SDL is in-service (due to recovery action, internal/external to this procedure) so this procedure is not appropriate; RETURN to the calling procedure.
- If the state is **OOS-MTCE-DSBLD**, CONTINUE with Step 51.
- If the state is **OOS-MTCE-FAF**, SKIP to Step 52.
- If the state is **OOS-MTCE-FE**, SKIP to Step 52.
- For any other state, SEEK TECHNICAL ASSISTANCE according to local practices.

51. The SDL port has been manually removed (unconditionally), and the port should be restored manually. Issue the input message:

RST:TRK,NEN=a-b-x-s-y-g-m-c,UCL

on an MCC/STLWS, where **a-b-x-s-y-g-m-c** is the SDL NEN in the form previously noted.

When the restoration is completed, RETURN to Step 50 for re-evaluation.

52. The SDL is OOS due to a DNU-S hardware/facility failure. Therefore, display the **1510,b,a DNUS b STATUS** page on an MCC/STLWS, where **b** is the DNU-S number (derived from the target NEN) and **a** is its GSM number.

Observe the status of DNU-S common control (**DNUSCC**), the DNUS common data (**DNUSCD**), and the STS-1 facility interface (**SFI**), where the DNUSCDs or SFIs to be investigated are associated with the data group (DG) identified in the NEN.

Proceed according to the following:

- If **both DNUSCCs** are OOS, indicating a duplex failure, CONTINUE with Step 53. Start with the repair of DNUSCC 0.
- If **both DNUSCDs** associated with data group **x** are OOS, indicating a duplex failure, SKIP to Step 61. Start with the repair of DNUSCD 0.
- If **both SFIs** associated with data group **x** are OOS, indicating a duplex failure, SKIP to Step 69. Start with the repair of SFI 0.
- Otherwise, SKIP to Step 77.

53. For the DNUSCC side **z** chosen, determine a detailed status by issuing the input message:

OP:CFGSTAT,SM=a,OOS,NOFE

where **a** is the target GSM number.

- If the state is **OOS-MAN-RMV**, CONTINUE with Step 54.
- If the state is **OOS-AUTO-RMV**, SKIP to Step 56.
- If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 57.
- If the state is **OOS-MAN-EX**, SKIP to Step 57.
- If the state is **OOS-REX-RMV**, SKIP to Step 58.
- If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 59.
- If the state is **OOS-AUTO-TBLA**, SKIP to Step 60.

54. Restore the DNUSCC, by using the menu selection **30z** on the 1510 MCC page, or the input message:

RST:DNUSCC=a-b-z

on an MCC/STLWS, where **a** is the GSM target number, **b** is the DNU-S number, and **z** is the DNUSCC side.

55. Did the DNUSCC restore successfully?

- If **yes**, RETURN to Step 50.
- If **no**, RETURN to Step 53.

56. The DNUSCC has been automatically removed for the purpose of running diagnostics. Allow the diagnostic to be scheduled because a fault has been detected by fault recovery. After the diagnostic completes, RETURN to Step 52.

57. The DNUSCC is currently being diagnosed, or manually exercised.

Allow automatic diagnostics to complete and then RETURN to Step 52.

Since this is a DNUSCC duplex failure recovery, interactive exercise/manual diagnostics should be stopped/aborted immediately, unless the diagnostic activity is part of a current repair procedure. Issue the

input message:

STP:DNUSCC=a-b-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, and **z** is the DSUSCC side.

If this request fails, use

ABT:DNUSCC=a-b-z

and then RETURN to Step 52.

58. The DNUSCC is currently being routinely exercised. Since this is a DNUSCC duplex failure recovery, routine exercise should be stopped immediately, using the input message:

STP:DNUSCC=a-b-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, and **z** is the DNUSCC side. RETURN to Step 52.

59. The DNUSCC is faulty. Find the most recent printed trouble location procedure (TLP) list on the ROP. Use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS®-2000 Switch" in the 235-105-220, *5ESS®-2000 Switch Corrective Maintenance Procedures Manual*. When the repair is completed, including the attempted restoration of the DNUSCC, is the DNUSCC successfully restored?

— If **yes**, RETURN to Step 50.

— If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure for the affected DNUSCC.

If DNUSCC 0 is being processed, RETURN to Step 53 to attempt the repair of DNUSCC 1, if DNUSCC 1 is still OOS.

60. The DNUSCC is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure for the affected DNUSCC.

If DNUSCC 0 is currently being processed, RETURN to Step 53 to attempt the repair of DNUSCC 1, if DNUSCC 1 is still OOS.

61. For the DNUSCD side **z** chosen, determine a detailed status by issuing the input message:

OP:CFGSTAT,SM=a,OOS,NOFE

where **a** is the target GSM number.

— If the state is **OOS-MAN-RMV**, CONTINUE with Step 62.

— If the state is **OOS-AUTO-RMV**, SKIP to Step 64.

— If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 65.

— If the state is **OOS-MAN-EX**, the state is **OOS-MAN-EX**

— If the state is **OOS-REX-RMV**, SKIP to Step 66.

— If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 67.

— If the state is **OOS-AUTO-TBLA**, SKIP to Step 68.

62. Restore the DNUSCD, by using the menu selection **31xz** on the 1510 MCC page, or the input message:

RST:DNUSCD=a-b-x-z

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the DNUSCD side.

63. Did the DNUSCD restore successfully?

— If **yes**, RETURN to Step 50 to re-evaluate SDL status.

— If **no**, RETURN to Step 61.

64. The DNUSCD has been automatically removed for the purpose of running diagnostics. Allow the diagnostic to be scheduled, because a fault has been detected by fault recovery. After the diagnostic completes, RETURN to Step 50.

65. The DNUSCD is currently being diagnosed, or manually exercised.

Allow automatic diagnostics to complete and then RETURN to Step 52.

Since this is a DNUSCD duplex failure recovery, interactive exercise/manual diagnostics should be stopped/aborted immediately, unless the diagnostic activity is part of a current repair procedure. Issue the input message:

STP:DNUSCD=a-b-x-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the DSUSCD side.

If this request fails, use

ABT:DNUSCD=a-b-x-z

and then RETURN to Step 61.

66. The DNUSCD is currently being routinely exercised. Since this is a DNUSCD duplex failure recovery, routine exercise should be stopped immediately, using the input message:

STP:DNUSCD=a-b-x-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the DSUSCD side.

If this request fails, use

ABT:DNUSCD=a-b-x-z

then RETURN to Step 50.

67. The DNUSCD is faulty. Find the most recent printed trouble location procedure (TLP) list on the ROP. Use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS[®]-2000 Switch" in the 235-105-220, *5ESS[®]-2000 Switch Corrective Maintenance Procedures Manual*. When the repair is

completed, including the attempted restoration of the DNUSCD, is the DNUSCD successfully restored?

- If **yes**, RETURN to Step 50 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure for the affected DNUSCD.

If DNUSCD 0 is being processed, RETURN to Step 61 to attempt the repair of DNUSCD 1, if DNUSCD 1 is still OOS.

68. The DNUSCD is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure, but if DNUSCD 0 is currently being processed, RETURN to Step 61 to attempt the repair of DNUSCD 1, if DNUSCD 1 is still OOS.
69. For the SFI side **z** chosen, determine a detailed status by issuing the input message:

OP:CFGSTAT,SM=a,OOS,NOFE

where **a** is the target GSM number.

- If the state is **OOS-MAN-RMV**, CONTINUE with Step 70.
- If the state is **OOS-AUTO-RMV**, SKIP to Step 72.
- If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 73.
- If the state is **OOS-MAN-EX**, SKIP to Step 73.
- If the state is **OOS-REX-RMV**, SKIP to Step 74.
- If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 75.
- If the state is **OOS-AUTO-TBLA**, SKIP to Step 76.

70. Restore the SFI, by using the menu selection **32xz** on the 1510 MCC page, or the input message:

RST:SFI=a-b-x-z

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the SFI side.

71. Did the SFI restore successfully?
 - If **yes**, RETURN to Step 50 to re-evaluate SDL status.
 - If **no**, RETURN to Step 69.
72. The SFI has been automatically removed for the purpose of running diagnostics. Allow the diagnostic to be scheduled because a fault has been detected by fault recovery. After the diagnostic completes, RETURN to Step 50.
73. The SFI is currently being diagnosed, or manually exercised.

Allow automatic diagnostics to complete and then RETURN to Step 69.

Since this is a SFI duplex failure recovery, interactive exercise/manual diagnostics should be stopped/aborted immediately, unless the diagnostic activity is part of a current repair procedure. Issue the

input message:

STP:SFI=a-b-x-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the SFI side.

If this request fails, use

ABT:SFI=a-b-x-z

and then RETURN to Step 61.

74. The SFI is currently being routinely exercised. Since this is an SFI duplex failure recovery, routine exercise should be stopped immediately, using the input message:

STP:SFI=a-b-x-z

on an MCC/STLWS, where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the SFI side.

If this request fails, use

ABT:SFI=a-b-x-z

and then RETURN to Step 50.

75. The SFI is faulty. Find the most recent printed TLP list on the ROP. Use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS®-2000 Switch" in the 235-105-220, *5ESS®-2000 Switch Corrective Maintenance Procedures Manual*. When the repair is completed, including the attempted restoration of the SFI, is the SFI successfully restored?

— If **yes**, RETURN to Step 50 to re-evaluate SDL status.

— If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure for the affected SFI.

If SFI 0 is being processed, RETURN to Step 69 to attempt the repair of SFI 1 (if SFI 1 is still OOS).

76. The SFI is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure for the affected SFI.

If SFI 0 is currently being processed, RETURN to Step 69 to attempt the repair of SFI 1 (if SFI 1 is still OOS).

77. Display the **1510,b,a DNUS b STATUS** page on an MCC/STLWS, where **b** is the DNU-S number (from the target NEN) and **a** is its GSM number.

Observe the status of the **TMUX**, and SONET terminating equipment (**STE**) facility, including the type of carrier group alarm (**CGA**). The TMUX/STE row to consider is the three-digit **STS indicator xsy**, where **x** is the data group, **s** is the STE, and **y** is the STS field in the target NEN. Also, note the status of the **spare TMUX** (the last TMUX in the target DG).

Proceed according to the following:

— If **TMUX** serving the target STS facility is **OOS**, SKIP to Step 78.

— If there is a **CGA** present on the target STE facility, SKIP to Step 85.

- If the affected **STE** is OOS (no CGA and parent TMUX is ACT), SKIP to Step 86.
- Otherwise, SKIP to Step 88.

78. For the OOS TMUX chosen, determine a detailed status by issuing the input message:

OP:CFGSTAT,SM=a,OOS,NOFE

where **a** is the target GSM number.

- If the state is **OOS-MAN-RMV**, SKIP to Step 79.
- If the state is **OOS-AUTO-RMV**, SKIP to Step 81.
- If the state is **OOS-MAN/AUTO-DGN**, SKIP to Step 82.
- If the state is **OOS-MAN-EX**, SKIP to Step 82.
- If the state is **OOS-AUTO/MAN-FLT**, SKIP to Step 83.
- If the state is **OOS-AUTO-TBLA**, SKIP to Step 84.

79. Restore the TMUX by using the menu selection **33xz** on the 1510 MCC page, or the input message:

RST:TMUX=a-b-x-z

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **z** is the TMUX number in the range 0-5 (corresponding to the STS indicator associated with the target NEN).

80. Did the TMUX restore successfully to ACT?

- If **yes**, RETURN to Step 50 to re-evaluate SDL status.
- If **no**, RETURN to Step 78.

81. The TMUX has been automatically removed for the purpose of running diagnostics. Allow the diagnostic to be scheduled because a fault has been detected by fault recovery. When the diagnostic completes, RETURN to Step 50.

82. The TMUX is currently being diagnosed, or manually exercised. When the diagnostic completes, or an interactive exercise session is stopped, RETURN to Step 50.

83. The TMUX is faulty. Find the most recent printed TLP list on the ROP. Use the procedure "Clear Diagnostic Failure in Hardware (Units/Circuits) of 5ESS®-2000 Switch" in the 235-105-220, *5ESS®-2000 Switch Corrective Maintenance Procedures Manual*. When the repair is complete, including the attempted restoration of the TMUX, is the TMUX successfully restored to ACT?

- If **yes**, RETURN to Step 50 to re-evaluate the impact on the SDL.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure for the affected TMUX.

If the **spare TMUX** is OOS, RETURN to Step 78 to attempt recovery of that unit.

84. The TMUX is in a trouble analysis state (repeated fault recovery removals, but diagnostics pass). SEEK TECHNICAL ASSISTANCE according to local procedure for the affected TMUX.

If the **spare TMUX** is OOS, RETURN to Step 78 to attempt recovery of that unit.

85. If the STE facility is experiencing a CGA (data from the 1510 MCC page indicates whether the alarm is local, remote, or an alarm indication signal), consult experienced transmission specialists, because the problem is probably in non-SM equipment. SEEK TECHNICAL ASSISTANCE according to local procedure.

Once the CGA is cleared, reenter this procedure to re-evaluate the effect on the target SDL.

86. Restore the affected OOS STE facility, using the menu selection **34xy** on the 1510 MCC page, or the input message:

RST:STEFAC=a-b-x-s

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, and **s** is the STE facility number (in the target NEN).

87. Did the STE facility restore successfully to ACT?

- If **yes**, RETURN to Step 50 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

88. From the 1510 page, display the **1511,b,y DNUS b STS xsy** page on an MCC/STLWS, where **b** is the DNU-S number, and **xsy** is the synchronous transport signal (STS) facility indicator, described in Step 77.

Check the status of the **STS**, **VT1.5** and **DS1** facilities, associated with the **VT1.5** number in the NEN, including the type of VT1.5 or DS1 carrier group alarm (CGA). The VT1.5 or DS1 facility is identified by a two-digit number **gm**, where **g** is the VT1.5 group and **m** is the VT1.5 member in the target NEN.

Proceed according to the following:

- If the affected **STS facility** is OOS, SKIP to Step 89.
- If there is a **CGA** present on the target VT1.5 or DS1 facility, SKIP to Step 91.
- If the affected **VT1.5 facility** is OOS (not OOSF and no CGA), SKIP to Step 92.
- If the affected **DS1 facility** is OOS (not OOSF), SKIP to Step 94.
- If the affected **DS1 facility** is **DGR** and the SDL status is **OOS-MAN-FE**, SKIP to Step 96.
- If none of the above, RETURN to Step 50 to re-evaluate SDL status.

89. Restore the affected OOS STS-1 facility, using the menu selection **3000** on the 1511 MCC page, or the input message:

RST:STSFAC=a-b-x-s-y

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, **s** is the STE number, and **y** is the STS number in the target NEN.

90. Did the STS facility restore successfully to ACT?

- If **yes**, RETURN to Step 50 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

91. If the VT1.5 or DS1 facility is experiencing a CGA (data from the 1511 MCC page indicates whether the alarm is local, remote or an alarm indication signal), consult experienced transmission specialists, because the problem is probably in non-SM equipment. SEEK TECHNICAL ASSISTANCE according to local procedure.

Once the CGA is cleared, reenter this procedure to re-evaluate the effect on the target SDL.

92. Restore the affected OOS VT1.5 facility, using the menu selection **31gm** on the 1511 MCC page, or the input message:

RST:VT1FAC=a-b-x-s-y-g-m

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, **s** is the STE number, **y** is the STS number, **g** is the VT1.5 facility group, and **m** is the VT1.5 facility member in the target NEN.

93. Did the VT1.5 facility restore successfully to ACT?

- If **yes**, RETURN to Step 50 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

94. Restore the affected OOS DS1 facility using the menu selection **32gm** on the 1511 MCC page, or the input message:

RST:DS1SFAC=a-b-x-s-y-g-m

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, **s** is the STE number, **y** is the STS number, **g** is the VT1.5 facility group, and **m** is the VT1.5 facility member in the target NEN.

95. Did the DS1 facility restore successfully to ACT?

- If **yes**, RETURN to Step 50 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

96. The affected DS1 facility is degraded (DGR) from a previous failed removal attempt. Therefore, restore the degraded facility using the menu selection **32gm,UCL** on the 1511 MCC page, or the input message:

RST:DS1SFAC=a-b-x-s-y-g-m,UCL

where **a** is the target GSM number, **b** is the DNU-S number, **x** is the DG number, **s** is the STE number, **y** is the STS number, **g** is the VT1.5 facility group, and **m** is the VT1.5 facility member in the target NEN.

97. Did the DS1 facility restore successfully to ACT?

- If **yes**, RETURN to Step 50 to re-evaluate SDL status.
- If **no**, SEEK TECHNICAL ASSISTANCE according to local procedure.

98. **STOP. YOU HAVE COMPLETED THIS PROCEDURE.**

GLOSSARY

This section provides acronyms, terms, and abbreviations used in this manual.

2ASTP

number 2A Signal Transfer Point

2SCCS

number 2 Switching Control Center System

2STP

number 2 Signal Transfer Point

30MPR

30-minute Marginal Performance Report

3B20D/3B21D

The Lucent Technologies 3B20 or 3B21 Duplex Computer, which is an equipment grouping that is also known as an administrative module (AM). The AM consisting of control units (CU), disk file controllers (DFC), disk drives, main stores (MAS), and input output processor (IOP), which together control the overall operation of a 5ESS[®]-2000 switch.

3BI

3B20D/3B21D computer Interface

3BRTR

3B20D/3B21D computer Real-Time Reliable

5E11

Software Release

The eleventh software release version of the 5ESS[®]-2000 switch. Includes changes and added features that can be found in the 5ESS[®]-2000 Switch Feature Handbook.

5E12

Software Release

The twelfth software release version of the 5ESS[®]-2000 switch. Includes changes and added features that can be found in the 5ESS[®]-2000 Switch Feature Handbook.

5E13

Software Release

The thirteenth software release version of the 5ESS[®]-2000 switch. Includes changes and added features that can be found in the 5ESS[®]-2000 Switch Feature Handbook.

5E14

Software Release

The fourteenth software release version of the 5ESS[®]-2000 switch. Includes changes and added features that can be found in the 5ESS[®]-2000 Switch Feature Handbook.

5ODA

5ESS[®]-2000 switch Office Data Administration

ABT

Abatement Threshold

This is the threshold for abating (ending) a message or process. If there are more than one abatement threshold; they may be labeled in the data base as **ABT1, ABT2, and ABT3**.

AC

Automatic Callback

This is a feature of the Local Area Signaling Service (LASS) that provides the calling terminal with the ability to place a call to the last incoming call directory number without having to redial the number.

ACC

Access Code

ACCL

Automatic Congestion Control Level

This is a parameter used in the release and address complete message to indicate to the 5ESS®-2000 switch that there is traffic congestion in the calling path. The automatic congestion control level parameter serves the same purpose as the dynamic overload control parameter.

ACCS

Automated Calling Card Service

These are various voice and data connection services offered to calling card holders.

ACD

Automatic Call Distributor

ACG

Automatic Call Gap

The ACG is used for controlling certain number service calls and software defined network (SDN) calls as they are being processed by the Service Switching Point (SSP) feature.

ACM

Address Complete Message

The address complete message is an SS7 message sent from the terminating office to indicate that the address information has been received, and call completion steps are to be performed by the terminating office.

ACNR UCL

Automatic Ring Recovery Indicator

This indicator on MCC Page 118 indicates that the DLN has been unconditionally restored.

ACP

Action Control Point

The 5ESS®-2000 switch serves as an action point for the software defined network and interfaces with the network control point data base.

ACQS

Automated Charge Quotation System

ACT

ACTive

ACU

Automatic Calling Unit

ADC

Address Complete

This is a message returned to the originating office of an SS7 call indicating that the called number and other connection requirements have been verified.

AFA

Analog Facility Access

This is a point in the 5ESS®-2000 switch configuration for accessing analog facilities.

AIM

Application Integrity Monitor

AIN

Advanced Intelligent Network

AIOD

Automatic Identification of Outward Dialing

Refers to the automatic identification of private branch exchange (PBX) stations that originate detailed billed calls.

AIS

Automatic Intercept System

ALM

Alarm

Any audible or visual indication used to call attention to an abnormal or trouble condition.

ALT

ALTernate

AM

Administrative Module

The part of the 5ESS®-2000 switch which performs call processing, administration, and maintenance which cannot be economically distributed to the switching modules. The AM consists of the processor, disk storage, and tape backup units. The AM processor performs the centralized processing functions, high-speed tape, and controls the flow of data between the other dedicated processors distributed throughout the remaining units. The processor functions are fully duplicated (except for the port switch) in order to assure continued processing capability.

AMA

Automatic Message Accounting

AMPS

Advanced Mobile Phone Service

Also referred to as *AUTOPLEX*®.

ANI

Automatic Number Identification

ANM

ANswer Message

The answer message is an ISUP message sent in the backward direction when the called party answers the phone.

ANNC

ANNouncement Channel

ANS

ANSwer

AP

Application Processor

AP

Attached Processor

AP30

Attached Processor 30

APC

Alias Point Code or Adjacent Point Code

This is a point code that represents mated STPs in the common channel signaling (CCS) network. Each of the STPs recognizes the alias point code and performs global title translations. These are used to assist in CCS network load balancing when signaling links fail or when one STP of a mated pair fail. (See capability code for LEC networks.)

APT

Automatic Process Testing

AR

Automatic Recall

This is a feature of LASS that allows the calling terminal to automatically place a call to the last party called from the calling terminal.

ARR

Automatic Ring Recovery

This is a subsystem used for diagnosing the CNI ring, and initiating a restart or recovery.

ARS

Automatic Route Selection

AS

Administrative Service Subsystem

ASIC

Application-Specific Integrated Circuit

An integrated circuit designed to perform a particular function by defining the interconnection of a set of basic circuit building blocks drawn from a library provided by the circuit manufacturer.

ASCII

American Standard Code for Information Interchange

A standard 8-bit code used for exchanging information among data processing systems and associated equipment.

ASE

Application Service Element

ASL

Analog Signaling Links

A CCS signaling link using analog facilities and when used with the 5ESS[®]-2000 switch operates on 4.8 kb/s.

ASN

Advanced Services Network

ASP

Advanced Services Platform

AT

Access Tandem

This is a tandem office in a LATA where inter-LATA carriers can access the local telephone service in that LATA.

ATF

ASCII Translation File

ATP

Access Transport Parameter

The access transport parameter (ATP) is an envelope provided in ISDN for the transport of Q.931 information elements transparently through the network.

ATP

All Tests Pass

AUD

AUDits

Audits are a collection of programs to monitor the occurrence of errors and inconsistencies encountered in the application software.

AUTO

AUTOMATIC

AUTOVON

AUTOMATIC VOICE Network

AVL

AVAILable

This is a term used in display messages to indicate the equipment, software, or circuit paths that are available

for service.

BAT

Backplane Attached Terminator

A printed circuit board that performs the DSU/CSU functions for digital data service (DDS) networks.

BC

Bearer Capability

BCD

Binary Code Data

BCI

Backward Call Indicator

BCID

Business Customer IDentification

Bellcore

Bell Communications Research

BISO

Begin ISolation

This is used to designate the CNI node that is located at the beginning of an isolated segment of the ring. This node is not part of the isolated segment, but is the point where the two channels of the ring are looped back to form the isolated segment.

BLA

BLocking Acknowledgement message

BLK

BLockEd

BLO

BLocking message

BM

Banded Messages

Banded messages are signaling messages for trunks using the CCIS6 signaling protocol. A band equates to a trunk group.

BN

Billing Number

BND

Billing Number Delivery

BNM

Band NuMber

BNS

Billing Number Screening

This is a parameter used with SS7 ISDN User Part protocol.

BOC

Bell Operating Company

BP

Banded Protocol

All CCIS6 trunk- and circuit-related messages use the CCIS6 banded protocol for routing through the CCS network. These banded messages are sent over preassigned signaling paths. The functions of CCIS6 banded protocol are as follows:

- Band translation at signal transfer points
- Routing of banded (trunk- or circuit-related) messages
- CCS signaling network management
- Circuit network management for CCIS6 trunks.

BRCS

Business and Residence Custom Services

The 5ESS[®]-2000 switch software that makes revenue generating features available to both business and residential customers.

BRI

Basic Rate Interface

Provides data and voice communications, simultaneously, plus circuit-switched and packet-switched services, with the use of two 64 kb/s B-channels and one 16 kb/s D-channel (2B+D). The BRI serves small-end systems such as voice-data workstations, multibutton voice stations, and terminal adapters for non-ISDN devices. Also known as **Digital Subscriber Line** in the ISDN network.

BVA

Billing Validation Application

This is a parameter used in the SS7 ISDN User Part protocol process.

BVD

Busy Verify Data

BWM

Broadcast Warning Message

CAC

Carrier Access Code

CADN

Circuit ADministration

CAMA

Centralized Automatic Message Accounting

This is an automatic message accounting system that provides call billing for more than one telephone company office. The CAMA feature in the 5ESS[®]-2000 switch permits the switch to collect and store toll information and message unit billing data on CAMA calls originated by a local office served by the CAMA office.

CAR

Computer Access Restriction

A term used to describe a switching office that handles inter-LATA traffic.

Carrier

A term used to describe a switching office that handles inter-LATA traffic.

CAS

Customer Account Service

CAS

Channel Associated Signaling

CC

Capability Code

This is a point code that represents mated STPs in the local exchange carrier (LEC) CCS network. Each of the STPs recognizes the capability code and performs global title translations. These are used to assist in CCS network load balancing when signaling links fail or when one of a pair of mated STPs fail. (See Alias Point Code for Common Channel Signaling Network.)

CC

Country Code

CCC

Commercial Credit Card

CCIS

Common Channel Interoffice Signaling System

An interoffice signaling scheme in which address and supervision signaling for trunks is carried over a data network rather than over the associated trunk.

CCIS6

Common Channel Interoffice Signaling System number 6

This is a signaling message format that conforms to the CCITT signaling system number 6.

CCIS7

Common Channel Interoffice Signaling System number 7

CCITT

Comite Consultatif International Telegraphe et Telephone

(International Telegraph and Telephone Consultative Committee) This is an international communications committee whose responsibility is to develop standard methods for telecommunications in order to interconnect between telecommunications networks. See ITU-TS.

CCITT7

Comite Consultatif International Telegraphe et Telephone signaling system 7

CCM

Common network interface Critical node recovery Monitor

CCR

Continuity Check Request

CCS

Common Channel Signaling

An operating capability of the 5ESS[®]-2000 switch software release program that is compatible with the CCIS6, ECIS6, DSIS6, SS7, and CCITT message protocols and permits the 5ESS[®]-2000 switch to access the CCS network.

CCS6

Common Channel Signaling system 6

CCS7

Common Channel Signaling system 7

This is a North American region version of CCITT7.

CCSINIT

CCS Initialization Process

The CCSINIT is a process that runs at RTR level 12. The CCSINIT, in turn, is responsible for creating two other initialization and recovery processes. The first of these created processes is the CNIINIT which is a part of the CNI/IMS package that is responsible for initialization of the CNI/IMS system.

CCSLK

CCS Signaling Link (for 5ESS[®]-2000 switch VCDX office)

CCSLKOFFN

SM status: one or more CCSLKs are off normal

CCSMDOFFN

SM status: the intra-SM MD link is not active

CD

Carrier Detect

CDBS

Customer Defined Bill Segmentation

CDGT

CalleD party Global Title

CDI

CoDe Index

CDMA

Code Division Multiple Access

CDO

Community Dial Office

CDPC

CalleD party Point Code

CdPN

Called Party Number

CDSN

CalleD party Subsystem Number

CDSP

CCIS6 Direct Signaling Protocol

Messages not related to circuits or trunks are called direct signaling messages and are routed over the CCS network using direct signaling protocol. These messages are not restricted to preassigned signaling paths, and can be injected into the network at any point, and are routed using destination addresses.

CDT

CalleD party Translation type

CF

Control Fanout

CFB

Call Forwarding Busy

CFBL

Call Forwarding Busy Line

CFDA

Call Forwarding Don't Answer

CFN

ConFusioN message

CFNR

Call Forward No Reply message

CFR

Configuration Fault Recovery

CFU

Call Forwarding Unconditional

CFV

Call Forwarding Variable

CGA

Carrier Group Alarm

CGB

Circuit Group Blocking message

Message used in ISUP trunk maintenance function to indicate that a trunk group is blocked.

CGBA

Circuit Group Blocking Acknowledgement message

CGGT

CallinG party Global Title

CGPC

CallinG party Point Code

CgPS

Calling Party Subaddress

CGSN

CallinG party Subsystem Number

CGT

CallinG party Translation type

CGU

Circuit Group Unblocking message

CGUA

Circuit Group Unblocking Acknowledgement message

CHG

CHarGe number

CHI

Call History Information

CHN

CHaNnel

CHN

CHarge Number

CIC

Carrier Identification Code

CIC

Circuit Identification Code

The circuit identification code is used with the routing label to associate a signaling message with a particular circuit.

CID

Channel IDentification

CIP

Carrier Identification Parameter

CKF

Continuity checkK Failure

CLID

Calling Line IDentification

CLS

Combined Link Set

CLU

CLUster

CM

Communication Module

Hardware that provides the interface between the AM and the SM(s). In a multimodule office, the CM consists of the message switch and the TMS.

CM2

Communication Module 2

CMD

Command

CMDA

Code Division Multiple Access

CMP

Communication Module Processor

CMT

CCS Message Transport

CN

CENTREX Network

CN-ISVM

CENTREX Network-InterSwitch Voice Messaging

CN-G

CENTREX Network-Government

CN-S

CENTREX Network-Special

CND

Calling Number Delivery

This is a function of the LASS ICLID feature that delivers the calling number to the terminating customer station.

CNI

Common Network Interface

The CNI functions as a packet-switching system in the signaling network. The CNI is not a stand-alone switching system but requires configuration to an application, such as the 5ESS[®]-2000 switch. The CNI consists of several peripheral processors (RPCs and LNs) serially interconnected and a central processor that performs the basic operating system duties in a distributed I/O processing architecture.

CNI/IMS

Common Network Interface/Interprocess Message Switch

The CNI/IMS consists of a single 5ESS[®]-2000 switch cabinet that provides two types of ring nodes: RPCs and LNs. The CNI/IMS is connected to the AM via a dual serial channel and also interfaces with DDS facilities.

CNIINIT

Common Network Interface/Initialization

CNIS

Calling Number Identification Service

CNISHRLIB

Common Network Interface SHaRed LIbrary

CNP

Charge Number Parameter

This is a parameter in the SS7 initial address message which carries the address digits of the station to which the call is to be charged.

CNR

Critical Node Recovery

CO

Central Office

COEES

Central Office Equipment Estimation System

CONN

CONNect

COSTAR

Check Only Simultaneous Trunk conversion via Automatic Recent change

COT

COntinuity Test

COT

Customer-Originated Trace

This is a Local Area Signaling Service (LASS) feature that allows an end-user the ability to trace the origin of the last incoming call.

COTM

COnTinuity Message

This is a message used in the SS7 protocol to advise that a continuity check is required on a circuit that has been selected for routing a call.

CP

Circuit Pack

A circuit pack is a plug-in unit used as a convenient means for assembling, on a single mounting, one or more components (such as, capacitors, inductors, diodes, resistors, transistors, etc). The components are interconnected to perform one or more circuit functions (such as, amplification, gating, timing, etc.), required in a circuit.

CPC

Capability Point Code

CPE

Customer Premises Equipment

This term refers to equipment that the customer keeps on site.

CPG

Call ProGress message

CPN

Calling Party Number

This is a parameter in the SS7 initial address message that carries the address digits of the specific station set originating the call.

CPU

Control Processing Unit

CQM

Circuit Query Request

CQR

Circuit Query Response

CRA

Circuit Reservation Acknowledgement message

CRF

Continuity Recheck Failure

CRM

Circuit Reservation Message

CSI

Carrier Selection Information

CSOP

Controller Spooler Output Process

CSU

Channel Service Unit

A type of interface used to connect a terminal or computer to a digital medium in the same way that a modem is used for connection to an analog medium. Performs certain line-conditioning functions, ensures network compliance per FCC rules, and responds to loopback commands from the central office. Also ensures proper 1s density in transmitted bit stream and performs bipolar violation correction.

CTO

Continuity TimeOut

CTTU

Centralized Trunk Test Unit

An operations support system (OSS) providing centralized trunk maintenance through a data link. This allows switching control center maintenance personnel to perform remote trunk testing on a local switching office from a work station.

CU

Control Unit

Part of the administrative module (AM). Control units perform translations, billing, and other data processing functions that can best be performed on a centralized basis. They control the operation of a 5ESS®-2000 switch by sending messages to module controllers (MC) and time multiplexed switch (TMS) control. When an MC loses its memory, the active CU obtains a copy from disk file and sends it to the MC. A CU operates in an asynchronous manner — the active processor does virtually everything. Included in a CU are a 3B

administrative module (3B AM), direct memory access (DMA), main store controller, and dual serial channels.

CVR

Circuit Validation Test Response

This is a response message to circuit validation test made when setting up a call using ISDN User Part protocol.

CVT

Circuit Validation Test

This is a validation test made when setting up a call using ISDN-User Part Protocol.

DAA

Design Automation Assistant

DAA

Direct Agent Access

DACT

Deactivated

DAS

Digital Analysis Selector

DAT

Disconnect Acknowledge Timer

DB

Data Base

Electronically stored information which may be retrieved and updated via DBM interface primitives.

DCE

Data Communications Equipment

The devices and connections of a communications network that connect the communication circuit between the data source and destination (the Data Terminal Equipment or DTE). A modem is the most common kind of DCE.

DCHN

D-Channel Node

DCIS

Direct Common channel Interoffice Signaling

DCIS6

Destination-routed Common channel Interoffice Signaling system number 6

The DCIS6 interworking protocol provides an interface between the CCIS6 and SS7 signaling protocols to permit transporting CCIS6 direct signaling messages over SS7 signaling protocol links. The DCIS6 interfaces the CCIS6 direct signaling messages at the SS7 signaling connection control part (SCCP).

DCS

Digital Cellular Switch

DCTU

Directly Connected Test Unit

DDS

Digital Data Service

A nationwide service that allows interconnection and transport of data at speeds up to 64 kbps over a 4-wire circuit.

DDSBS

Duplex Dual Serial Bus Selector

A channel which permits the connection of two dual serial channels to a single I/O device.

DEL

DELeTe

DEN

Digital Equipment Number

DETL

Detail Report

DES

DEStination

DEST

DEStination

DF

Data Fanout

DFA

Digital Facility Access

This is a point of access to the digital facilities in the 5ESS[®]-2000 switch configuration.

DFC

Data File Controller

DFI

Digital Facility Interface

DFI2

Digital Facility Interface version 2

DGN

DiaGNostic

DGR

DeGRaded

DIP

Dual In-line Package

The most common type of package for small and medium scale integrated circuits, with up to about 48 pins. The pins hang vertically from the two long edges of the rectangular package, spaced at intervals of 0.1 inch. The pins fit through holes in the circuit board to which they are soldered, or plug into a socket.

DIR

DIRection

DIS

DIScard

This term is used in some messages and commands to indicate that a message or parameter is to be discarded.

DISC

DISConnect

DL

Digital Loopback

DLC

Digital Loop Carrier

DLN

Direct Link Node

This is a node on the CNI ring that performs signaling message processing normally performed by the 5ESS[®]-2000 switch 3B20D computer and interconnects with other nodes on the ring via the dual ring bus.

DLN30

Direct Link Node 30

DLN AP

Direct Link Node Attached Processor

This processor is used to process messages from the DLN to other processors and the communication module.

DLTU

Digital Line Trunk Unit

DMA

Direct Memory Access

Provides direct access to the main store by peripheral units without involving the administrative module. This is a method of transferring information directly to the main memory, bypassing the central control unit. This method does not require software to keep track of memory addresses and, therefore, greatly improves the transfer rate.

DMI

Discard Message Indicator

DMERT

Duplex MultiEnvironment Real Time

This is the 3B20 computer system software.

DN

Directory Number

A 7-digit telephone number made up of a 3-digit central office code plus a 4-digit station number.

DNHR

Dynamic Non-Hierarchical Route

DNP

Directory Number Privacy

This is a function of the LASS ICLID feature that allows the calling party to prevent the calling directory number from being delivered to the terminating station.

DNU

Digital Network Unit

DNU-S

Digital Network Unit - SONET

DNUSCC

Digital Network Unit - SONET Common Control

DNUSCD

Digital Network Unit - SONET Common Data

DOC

Dynamic Overload Control

This is a parameter used in the release and address complete messages in the SS7 ISDN User Part protocol to indicate to the 5ESS[®]-2000 switch of traffic congestion.

DOM

DOMestic

This is used in commands and message responses to indicate that a call is for domestic subscribers rather than an international call.

DOM

DOMain

DP

Dial Pulse

DPC

Data Port Circuit

DPC

Destination Point Code

A destination point code is any exchange/STP that terminates either CCSLKs or trunk routes directly, or other destinations within the regional network.

DRM

Distinctive Remote Module

DS

Direct Signaling

DS0

Digital Signal at level 0

A signal at 64 kb/s rate.

DS1

Digital Signal at level 1

A convention for pulse code modulated (PCM) signaling at a 1.554 Mb/s rate.

DSA

Dial Service Assistance

DSBLD

DiSaBLed

DSBS

Dual Serial Bus Selector

A channel that provides the capability to connect two serial channels (from duplex control units) to a single input/output device.

DSCH

Dual Serial CHannel

A bus in the CNI that provides packet data transfer between the RPCs, LNs, and the AM.

DSE

Data Base Search Event

This is an event used in OSPA call processing for searching various data bases to determine the proper handling and billing of calls. This signal is at 1.544 Mb/s rate.

DSIG

Direct SIGnaling status indicator

Direct signaling messages are messages that are related to circuits or trunks. These provide routing for noncircuit related messages, communications between CCS network services and functions, and network management procedures.

DSL

Digital Signaling Link

This signaling link uses digital facilities and operates at 56 kb/s. The part of the signaling link between the ring node and the transmission facility is made up of a TF5 or TF9 circuit pack (digital service adapter), and a digital service unit (DSU) used in conjunction with a channel service unit (CSU).

DSL

Digital Subscriber Line

DSN

Defense Switched Network

DSP

Direct Signaling Protocol

Messages not related to circuits or trunks are called direct signaling messages and are routed over the CCS network using direct signaling protocol. These messages are not restricted to preassigned signaling paths, and can be injected into the network at any point, and are routed using destination addresses.

DSU

Data Service Unit

A device used in digital transmission to connect a CSU to data terminal equipment (a terminal or computer) in the same way that a modem is used for connection to an analog medium. A DSU provides a standard interface to a user's terminal that is compatible with modems and handles such functions as signal translation, regeneration, reformatting, and timing. The transmitting portion of the DSU processes the customer's signal into bipolar pulses suitable for transmission over the digital facility. The receiving portion of the DSU is used to extract timing information and to regenerate mark and space information from the received bipolar signal.

DSU

Digital Service Unit

The mounting unit for digital service circuits (DSC). Depending upon the circuit packs inserted, it becomes either a local (LDSU) or global (GDSU) unit.

DSU2

Digital Service Unit model 2

DSX

Destination Switch complex

DTE

Data Terminal Equipment

A device that acts as the source and/or destination of data, and controls the communication channel. DTE includes computers, protocol converters, and multiplexers.

DTMF

Dual Tone MultiFrequency

A means of address signaling to the switching system that uses a simultaneous combination of one of a lower group of frequencies and one of a higher group of frequencies to represent each digit (1 through 0), character (A through Z), and symbol (* and #).

Dual Seizure

See "Glare"

DUR

DURation

EA

Exchange Access

This is a point where inter-LATA customers access the exchange to request connection across the network boundaries. This is sometimes referred to as "Equal Access."

EADAS

Engineering and Administration Data Acquisition System

This is one of the support systems used with the 5ESS[®]-2000 switch to monitor the performance of the switch and the CCS network.

EAE0

Equal Access End Office

This is an office in a LATA where all long distance companies and their customers can gain access to the local network.

EAI

Emergency Action Interface

The maintenance interface between a 3B control unit and a serial data link for executing various manual override functions, (such as, "force-on-line," "stop and switch," etc.

EAMF

Equal Access MultiFrequency

This is the in-band signaling used for exchange access calls.

EAR

Error Analysis and Recovery

ECD

Equipment Configuration Data

A data base that describes the physical and logical configurations (for example, interfaces of IOP and AM) of the 3B20D computer and peripheral hardware. It also contains configuration and control information for the audit and craft interface software system.

ECIS

Embedded Common channel Interoffice Signaling

ECIS6

Embedded Common channel Interoffice Signaling system number 6

The ECIS6 interworking protocol is used for transmitting CCIS6 banded messages using the link level of the SS7 signaling protocol message transfer part. This protocol allows the 2STP CCS network to use 56 kb/s signaling links and build up the signaling capacity. The ECIS6 interworking protocol follows SS7 transport capability at the link level, but follows the CCIS6 banded message routing at the network level.

ECP

Executive Control Processor

EDSL

Extended Digital Subscriber Line

Egress

Describes a call leaving a toll network and entering the local network.

EIA

Electronic Industrial Association

EIS

External Information System

EISO

End ISolation

This term refers to a node on the CNI ring that designates the end of an isolation segment of the ring. The node is not part of the isolation segment.

EMER

EMERgency

EMR

EMergency Restart

EO

End Office

The EO is a LEC switch that serves a customer on a call. The originating EO serves the calling party. The terminating EO serves the called party. The EO may also support trunks that go to other offices.

ESAC

Electronic Switching Assistance Center

EXCP

EXCePtion

EXM

EXit Message

This is a message used in SS7 signaling to indicate to the end office that an initial address message has been sent by the Access Tandem to the toll office for an inter-LATA call.

EXM-2000

Extended Switch Module-2000

FA

Fuse Alarm

FAC

Facility Administration and Control

FAF

Facility Failure

FC

Feature Control

A software subsystem that sequences call processing actions at a hardware independent level.

FCA

Fully Coded Addressing

This is a CCS single-stage protocol used to route international outbound calls in a uniform simple format throughout the AT&T Communications domestic network. The signaling messages for the international calls are routed through the CCS network between the 5ESS[®]-2000 switch toll office and the 4ESS[™] switch at the international service center.

FCC

Federal Communications Commission

FCI

Forward Call Indicator

FCI is a parameter that is present in the ISUP IAM message and is used to provide information to the terminator about the originating party.

FDB

Feature Data Block

FGB

Feature Group B

FGD

Feature Group D

FLTY

FauLTY

FPCR

Full Point Code Routing

FPI

Full Process Initialization

FRJ

Facility ReJect message

FTSP

Final Translation Signaling Point

FX

Foreign Exchange

GAP

Generic Address Parameter

GDSU

Global Digital Service Unit

GETS

Government Emergency Telecommunications Service

Glare

This is a dual seizure of a transmission or signaling path. The path is seized from both ends, simultaneously.

Global Title

This is an address information used in by the CCS network for determining the routing of signaling messages and call destinations.

Global Title Translations

The global title translation is a process of determining from the global title information (dialed digits and translation type) the destination point code and subsystem number for the data base being addressed for call completion.

GN

Generic Name

GRA

Group Reset Acknowledgement message

GRS

Group ReSet

This is a message used in the SS7 ISDN User Part protocol for resetting a complete trunk group.

GSM

Global Switching Module

A global SM is an SM that contains the PSU platform that terminates CCS signaling links (CCSLKs). When an ordinary 5ESS[®]-2000 switch VCDX office is converted to a VCDX office with CCS7 access on a PSU, the VCDX SM/SM-2000 is the GSM.

GT

Global Title

GTT

Global Title Translation

HCGA

Hardware Carrier Group Alarm

HDLC

High Level Data Link Control

HFDT

History File Descriptor Table

HGB

Hardware Group Blocking

HGU

Hardware Group Unblocking

HPC

High Probability of Completion

HV

Hardware Version

HW

HardWare

I/O

Input/Output

IAM

Initial Address Message

The initial address message is an SS7 signaling message transmitted to select an outgoing circuit. This message equates to transmitting the routing digits through the voice path in an in-band signaling arrangement.

IC

Inter-local-access-transport-area Carrier

This is a company responsible for transmitting telecommunications messages between LATAs in the nationwide telecommunications network.

ICC

International Control Centre

ICCV

International Credit Card Verification

ICL

Inter-remote switching module Communications Links

ICLID

Individual Calling Line IDentification

This is a LASS feature that delivers the calling party's directory number to analog, basic rate interface, and primary interface users on voice calls.

ID

IDentification

IE

Information Element

IEs are Q.931 parameters used to transport data via ISUP messages.

IEC

InterExchange Carrier

An IEC can be an inter-LATA carrier or an international carrier.

IFB

InterFrame Buffer

II

II are the two information digits sent with ANI in an Exchange Access (EA) call.

IMS

Interprocessing Message Switch

Hardware and software in the switching module (SM) used to support OSPS, BRCS, CSDCII, and the ICLID for intra-office calls and 16 kb/s intra-office packet switching.

IMSDRV

Interprocessing Message Switch DRiVer

IMT

InterModule Trunk

A loop-around trunk from one SM to a *different* SM.

IN

Intelligent Network

INC

INternational Carrier

An international carrier is similar to an IC, but INCs only handle international traffic.

INF

INFormation message

INFO

INFORmation

INH

INHibit

INR

INformation Request

INT

INiTializing

INTL

INTernational network

Intra-IMT

Intramodule Trunk

Intermodule trunk that is looped within the *same* SM originating point code.

Intra-SM MD

Intra-Switching Module Message Delivery Link

INV

INValid

INWATS

Inward Wide Area Telephone Service

Calls to area code 800 subscribers from one or more predetermined geographical areas at a rate based on expected usage. These calls are toll free to the calling parties.

Input/Output

Input/Output is the process of transmitting information from an external source to an external destination.

IPCT

In Progress Call Trace

IRN2

Integrated Ring Node 2

IS

In Service

ISC

International Switching Center

ISDN

Integrated Services Digital Network

ISDN-UP

Integrated Services Digital Network-User Part

ISDN User-Network Interface Protocol

See Q.931 Protocol.

ISO

International Standards Organization

ISO

ISOLated

ISTF

Integrated Services Test Facility

ISU

Initial Signal Unit

ISUP

Integrated Services digital network User Part

ISUP7

Integrated Services digital network User Part with signaling system number 7 protocol

This is the protocol for handling ISUP messages and Q.931 messages over the SS7 network.

ISVM

Inter-Switch Voice Messaging

ITC

Independent Telephone Company

ITC

Information Transfer Capability

ITSP

Intermediate Translation Signaling Point

ITU

International Telecommunication Union

See ITU-TS.

ITU-TS

International Telecommunication Union - Telecommunication Standardization sector

As a result of the World Telecommunications Standardization Conference held March 1-12, 1993, the CCITT no longer exists as an organization under the International Telecommunication Union (ITU). According to the ITU, the CCITT is now referred to as the International Telecommunication Union - Telecommunication Standardization Sector (ITU-TS).

IUN

Interprocessing message switch User Node

This is an active node on the CN1 ring, but performs no signaling. This node provides the common circuitry on which link nodes (LNs) or direct link nodes (DLNs) are built.

KB

Kilobyte

Consists of 1024 bytes.

KP

Key Pulse

LASS

Local Area Signaling Service

This is a signaling service that supports features such as, Automatic Callback and Automatic Recall. This is done from the 5ESS[®]-2000 switch using the SS7 signaling protocol.

LATA

Local Access Transport Area

This is a geographical area used for defining the local exchange carrier territory.

LB

Library

LBLK

Locally Blocked

LBRV

Low Bit Rate Voice

This technique may be used over speech trunks. When present on a speech trunk, the underlying bit stream may be corrupted. Trunks which use this technique should be avoided when routing voiceband data calls.

L/C Network

Electrical network consisting of inductors and capacitors.

LCC

Line Class Code

LDIT

Local Digit Interpreter Table

LDP

Long Distance Platform

LDSU

Local Digital Service Unit

The part of the switching module (SM) that provides high-usage service circuits; such as, tone decoding, tone generation, conferencing, and voice-frequency testing.

LDSU2

Local Digital Service Unit model 2

LDSU2CTD

Local Digital Service Unit model 2 Centralized automatic message accounting Transfer Decoder

LDSU2TD

Local Digital Service Unit model 2 Tone Decoding

LDSU2TG

Local Digital Service Unit model 2 Tone Generator

LDSU2TX

Local Digital Service Unit model 2 Tone Transceiver

LEC

Local Exchange Carrier

This is a local operating telephone company furnishing service to individual business and private customers.

LED

Light Emitting Diode

LHB

Line History Block

This is a long retention block of data assigned to a customer's terminal which provides stored data required to allow the customer to activate the Automatic Callback and Automatic Recall features at any time after the last incoming call was received or the last outgoing call was dialed.

LI

Link Interface

The LI circuit pack is a single-port link interface board that terminates an SS7 link on a CNI ring. It supports an EIA RS-449 interface and functions as DTE.

LI4S

Link Interface

The LI4S circuit pack is a four-port link interface board. For SS7 applications, it may terminate a single SS7 link on a CNI ring. It supports a standard TTL interface and functions as DTE.

LICTSL

Local Interference Controlled by This Signaling Link

LIDB

Line Information Data Base

LINH

Locally Inhibited

LKER

Link Test Error

LL

Local Loop

LLC

Low Layer Compatibility

LN

Link Node

A part of the CNI that performs the message handling protocol, control functions, and self-diagnostics. The LN establishes the connection to the signaling network via A-links.

LNP

Local Number Portability

LOC

Local

LPA

LooPback Acknowledgement

Message from the call processing subsystem.

LPM

Last Period Measurement

LPN

Local Private Network

LRA

Library Request Administrator

LS

Link Set

LSF

Local area signaling service Selective Feature

MA-UUI

Message Associated User-to-User Information

This is information from a user to send user-defined data as part of the signaling information during setup and clearing of circuit-switched calls.

MAN

MANual

MASC

MAin Store Controller

MB

Megabyte

Consists of 1,048,576 bytes.

MBG

Multi-switch Business Group

MBGID

Multi-switch Business Group IDentification

MCC

Master Control Center

This is the control center of the 5ESS[®]-2000 switch office which consists of the I/O channel input and the receive-only printer. From this location office maintenance personnel monitor the switch processes and perform administrative and maintenance functions.

Message Mapping

This is the designed method of directing messages from one signaling point or protocol to another in the process of setting up or tearing down a telecommunications call.

MCNT

Message CouNT

MCTU2

Module Control and Time slot interchange Unit, model 2

MD

Message Delivery

MD PH

Message Delivery Protocol Handler

MDII

Machine Detected Interoffice Irregularities

MDL

Memory Data Link

MDST7

CCS channel group type in which MD and ST7 functions are handled by the same PH.

MF

MultiFrequency

MGB

Maintenance Group Blocking

MGSZE

MessaGe SiZE

MGU

Maintenance Group Unblocking

MINT

Multifarious Intra-Network Trunk

MLPP

Multi-Level Precedence Preemption

MML

huMan-Machine Language

MMRSM

Multi-Module Remote Switching Module

MMUM

Miscellaneous MultiUnit Messages

MOCT

Measurement Output Control Table

MOOS

Manual Out Of Service

MPR

Machine Performance Report

MROP

Maintenance Read-Only Printer

MRV

Message Routing Verification

MRVA

Message transfer part Routing Verification Acknowledgement

MRVR

Message transfer part Routing Verification Result

MRVT

Message transfer part Routing Verification Test

MSB

Message Sampling Board

This is a stand-alone piece of hardware that is inserted in a spare slot next to the LI to be monitored by the Message Sampling System (MSS).

MSC

Mobile Switching Center

MSKP

Message Switch Kernel Process

MSS

Message Sampling System

This is a noninterfering monitoring system used to monitor data transmitted between the CNI node processor and the link interface.

MSS

Message Service System

MSU

Message Signaling Unit

MTCE

Maintenance

MTP

Message Transfer Part

The message transfer part provides routing of messages through the CCS network using destination point codes. The destination point code identifies each signaling point with a network identifier, a cluster number, and member number. The destination point code routing is accomplished by use of message handling, signaling link management, and signaling route management functions.

MTSO

Mobile Telephone Switching Office

MTYPE

Message TYPE

MWI

Message Waiting Indicator

NAP

NAme Privacy

NAP

Network Access Point

NARTAC

North American Regional Technical Assistance Center

Nature of Address Indicator

A subfield of the ISDN user-network interface (Q.931) calling party information element. The nature of address indicator is based on the calling party number information element.

NC

Non-Conforming

NCD

Network Call Denial

Capability that enables a carrier switch to block inter-LATA calls from non-paying customers.

NCLK

Network Clock

The digital reference clock for the network. Provides time synchronization and uniform time stamping for all reports and messages across the network. Also provides time synchronization.

NCP

Network Control Point

A network control point (NCP) is an office in the CCS network containing detailed logic and data used to provide diversified calling services and features. Service related queries from offices in the CCS network are routed to an NCP where replies are formulated and returned to the originating offices. The NCP performs similar functions as the service control point (SCP). The NCP uses the 3B20D computer for message processing.

NCT

Network Control and Timing

NCT

Nuisance Call Trace

NEBS

Network Equipment Building Systems

NEMOS

Network Management Operation Support System

NEN

Network Equipment Number

NI

Network Interconnect

The connection of calls between the local exchange carrier and the inter-LATA or international carriers. (See SS7 ISUP Network Interconnect.)

NISDN

National Integrated Services Digital Network

NM

Network Management

NN

National Number

NNDA

Name Number Display Allowed

NNP

Name Number Privacy

NOC

Normalized Office Code

NP

Node Processor

NPA

Number Plan Area

NRM

Normal

NS

Network Systems

NS

Number Service

A specially-dialed number that accesses a special telecommunications service. The 800 service is an example of a number service.

NS800

Number Service 800

NSC

Network Service Complex

NSD

Network Services Division

NSEC

Network Switching Engineering Center

NTC

Network Trunk Congestion

NTW

Network

NXX

Local office exchange number

The office code part of the dialed digits.

OA&M

Operations, Administration, and Maintenance

OAT

Originating Access Tandem

An access tandem is an LEC switch that allows calls to be transported from EOs to ICs, IECs, and INCs. Access Tandems handle intra-LATA traffic as well. A switch serving as an access tandem may also have lines attached to it. In that case, the access tandem is considered an EO and the lines are known as colocated stations.

OBCI

Optional Backward Call Indicator

This is a parameter which may be present in an ISUP ACM or CPG message. This parameter is used to transport information about the terminating party back to the originating party over ISUP trunks.

OCAS

Operator services position system Customer Account Services

OCN

Original Called Number

OCSS

Operator services position system Common Channel Signaling

ODA

Office Data Administration

ODBE

Office Data Base Editor

ODD

Office Dependent Data

The data base, specific to a particular office, that contains unique trunk and line assignments; thereby, allowing the office to process call traffic.

OE

Office Equipment

OEO

Originating End Office

This is the office that the calling party's phone is connected to.

OFA

Operator services position system Facility Administration

OFL

OFF Line

OFR

Office Records

OFSTB

OFFSeT and Bit pattern

OLI

Originating Line Information

OM

Output Message

OMAP

Operations and Maintenance Applications Part

OOS

Out Of Service

The term used in display messages to indicate that equipment, software, or transmission facility is "out-of-service."

OOSF

Out Of Service Family of Equipment

OOST

Out Of Service Test

OOST

Out Of Service Transient

OP

Output

OPC

Originating Point Code

The 9-digit number (*ANSI*TM or AT&T format) associated with the signaling platform (CNI or GSM).

ORM

Optically-integrated Remote switching Module

OS

Operating System

OS

Operations System

OSDS

Operating System for Distributed Switching

OSI

Open System Interconnection

OSPS

Operator Services Position System

The OSPS uses features provided by a host *5ESS*[®]-2000 switch and dedicated peripheral equipment to support operator and attendant services.

OSPS T&A

Operator Service Position System Toll And Assistance

OSS

Operation Support System

Computer systems that may be used to provide additional administrative support; for example, the Engineering and Administrative Data Acquisition System (EADAS), the Central Office Equipment Report (COER), and the Switching Control Center System (SCCS).

OSX

Originating Switch complex

OTO

Originating Toll Office

This is the first switch within an IC/INC network to which a call is routed from the originating LATA.

OTP

Originating Terminal Process

If a switch were broken into two halves, the OTP is the half that handles routing, digit analysis, forward messages from the originator, and other duties associated with call originations.

PAS

Protected Application Segment

PBX

Private Branch eXchange

PC

Peripheral Controller

Circuitry in the input/output processor that interfaces with peripherals outside the 5ESS®-2000 switch AM.

PC

Point Code

PCBLA

Process Control Block Area

The PCBLA is an area of memory that contains global data. The CCS feature data block is part of this global data. When references are made to the PCBLA in this document, they usually mean the CCS feature data block which is a sub-area.

PCC

Pseudo Country Code

PCCP

Point Code Change Process

PCM

Pulse Code Modulation

A modulation scheme in which the signal waveform is sampled at regular intervals, quantized into discrete steps, and then transmitted over the system by means of a code pattern of a series of pulses.

PCN

Peripheral Controller Node

PDS

Program Documentation Standard

PF

Printout Follows

PF

Packet Fanout

PFA

Private Facility Access

PH

Protocol Handler

PH1

Protocol Handler model 1

PH3

Protocol Handler model 3

PH22

Protocol Handler model 22

PI

Packet Interface

PI2

Packet Interface Version 2

PIDB

Peripheral Interface Data Bus

PIFB

Padded InterFrame Buffer

PM

Plant Measurements

The 5ESS®-2000 switch generates a 24-hour plant report containing data regarding originated incoming and outgoing calls, customer dialing irregularities, and call setup troubles.

PMCR

Plant Measurement Count Report

POTS

Plain Old Telephone Service

Basic voice service via telephone.

PPC

Primary Point Code

PPCC

Pseudo-Point Code Capability

PRI

Primary Rate Interface

PRM

Processor Recovery Message

PRO

PRocess Outage

PROG

PROGress

PSD

Packet-Switched Data

PSLT

Periodic Signaling Link Test

PSTN

Public-Switched Telephone Network

PSU

Packet Switch Unit

PSU1

Packet Switch Unit Version 1

PSU2

Packet Switch Unit Version 2

PSUCOM

Packet Switch Unit COMMon circuits

PTS

Per-Trunk Signaling

PTW

Primary Translation Word

PWR

Power

Q.931

ISDN User-Network Interface Protocol

The term Q.931 is the identification of the CCITT recommendation for ISDN user-network interface protocol. It covers the procedure for establishing, maintaining, and clearing network connections at the ISDN user-network interface.

QTY

QuanTitY

QUSBL

Quarantine USaBLe

RAC

Ring Access Circuit bus

RAO

Revenue Accounting Office

RBLK

Remotely Blocked

RBOC

Regional Bell Operating Company

RC

Recent Change

This is a system function that allows maintenance personnel access to the 5ESS[®]-2000 switch data base. Recent change is used to add to or delete from data bases and update or verify the data base using the new select/mark format.

RC

Return Code

RCD

ReCorD

RCPTP

Recent Change of Protocol Timers and Parameters

RC/V

Recent Change and Verify Subsystem

This stand-alone package provides the maintenance personnel with the ability to maintain the office dependent data of the data base without the need for an operations support system.

RCV

Recent Change and Verify Subsystem

See RC/V.

RDL

Remote Digital Loopback

REL

RELease message

REMACS

REMOte ACcess Subsystem

REPT

Report

RES

RESume message

REST

REStart

RFR

Reason For Return

RGN

RedirectinG Number

RI

Redirection Information

RI

Ring Interface

RI

Route Index

RINGMON

RING MONitor

RINH

Remotely Inhibited

RIP

Redirection Information Parameter

RLC

ReLease Complete

RLN

Remote Local Network

RMAS

Remote Memory Access System

This is a subsystem used with local exchange carrier 5ESS[®]-2000 switch applications.

RMV

Remove

RN

Redirecting Number

RN

Ring Node

RNA

Ring Node Address

ROP

Receive-Only Printer

The printer used only for receiving messages at the Master Control Center.

Routing Label

Part of the signaling message used to route the message to a particular destination point over a specific circuit group.

RPC

Ring Peripheral Controller

A part of the common network interface (CNI) that transports signaling messages and internal control common network interface/interprocess message switch (CNI/IMS) messages between the administrative module (AM)

processor and the ring via a dual serial channel. The RPC node does not provide network connection. The 5ESS®-2000 switch uses two RPCs.

RPCN

Ring Peripheral Controller Node

A part of the CNI that transports signaling messages and internal control CNI/IMS messages between the AM processor and the ring via a dual serial channel. The RPC node does not provide network connection. The 5ESS®-2000 switch uses two RPCs on the CNI ring.

RPN

Remote Private Network

RPTERR

RePorT ERRor handler

RSC

ReSet Circuit message

RSM

Remote Switching Module

RSRC

Lack of internal switch resources

RST

Restore

RTA

Routing and Terminal Allocation

This subsystem is responsible for selecting an outgoing trunk when routing interswitch and also for selecting the appropriate terminating line.

RTAD

ReTurn Address

RTDSP

Real-Time DiSPlay

RTI

RouTing Index

RTR

Real-Time Rating

RTR

Real-Time Reliable

This is a control system for performing operations in time with a physical process to produce outputs for controlling the process. The *UNIX*® RTR system is used in the 5ESS®-2000 switch to generate various maintenance and administration reports.

RTS

Request To Send

RTU

Right To Use

RVT

Routing Verification Test

SAC

Service Access Codes

Service access codes such as 800, 888, or 887 initiate toll-free services.

SADC

Special Access Data Channel

SCA

Selective Call Acceptance

SCANS

Software Change Administration and Notification System

SCC

Switching Control Center

SCCP

Signaling Connection Control Part

This part provides additional functions to the MTP to cater for both connectionless and connection-oriented network services to transfer circuit related or noncircuit related signaling information and other types of information (that is, for management and maintenance purposes) between signaling nodes via a CCS network.

SCCS

Switching Control Center System

This is an automated switching system that enables a centralized group of technicians to perform functions and measurements at a remote location that would otherwise be performed at the MCC.

SCF

Selective Call Forwarding

SCGA

Software Carrier Group Alarm

SCP

Service Control Point

An SCP is an office in the CCS network containing detailed logic and data used to provide diversified calling services and features. Service related queries from offices in the CCS network are routed to an SCP where replies are formulated and returned to the originating offices. The SCP performs similar functions as the network control point (NCP).

SCR

Selective Call Rejection

SDA

Selective Distinctive Alerting

SDL

Signal Data Link

SDN

Software Defined Network

This is a feature that provides virtual private network capabilities for customers with multiple business locations.

SEP

Service Entry Points

SEP

Signaling End Point

SEPR

Signaling Equipment Performance Report

SERV

SERvice

SFG

Simulated Facilities Group

SFI

STSX-1 facility interface

SG

Service Group

SI

Service Information

SIM

System Integrity Monitor

SIO

Service Information Octet

SIP

Signal Interface Points

SLC

Signaling Link Code

SLE

Screen List Editing

SLK

Signaling Link

SLM

Signaling Link Management

This is the function of establishing and maintaining predetermined capability of the signaling links and restoration action when links fail.

SLMK

Signaling Link Monitor Kernel

This is an audit program that is concerned with the integrity of the CCS network.

SLS

Signaling Link Selection

SLT

Signaling Link Test

SM

Switching Module

The SM connects all external lines and trunks to the 5ESS[®]-2000 switch and handles most of the call processing tasks. The SM converts signals received from the lines and trunks into internal digital time-division format known to the office.

SM-2000

Switching Module-2000

SMH

Signaling Message Handler

SMHHOME

Signaling Message Handler Home

This is a message that is used to transmit the DLN status to the signaling nodes in the CNI ring.

SMHSTOP

Signaling Message Handler Stop

This is the message received by the nodes when the messages routed to the home DLN is halted.

SM MD

Switching Module Message Delivery

SMP

Switching Module Processor

SN-2000

Service Net-2000

SNFA

Shared Network Facility Agreements

SNM7

Signaling system number 7 Signaling Network Management Messages

SNPR

Signaling Network Performance Report

SNPR1

Signaling Network Performance Report part 1

SNPR2

Signaling Network Performance Report part 2

SONET

Synchronous Optical Network (High Speed Fiber)

SOP

Spooler Output Process

SOPC

Source Originating Point Code

SP

Signaling Point

SP

Switching Point

SP

Signal Processor

SPC

Secondary Point Code

SPI

Signaling Point Isolation

SRN

Signaling Routing Node

SRV

SCCP Routing Verification

SRVA

Signaling connection control part Routing Verification Acknowledgement

SRVR

Signaling connection control part Routing Verification Result

SRVT

Signaling connection control part Routing Verification Test

SS7

Signaling System number 7

This is a signaling message format that conforms to the CCITT signaling system number 7.

SS7 ISUP Network Interconnect

A capability that provides the means of connecting SS7 calls between the local exchange carrier and the inter-LATA or international carriers.

SSD

Second Start Dial

SSN

SubSystem Number

SSP

Service Switching Point

This feature enables the 5ESS[®]-2000 switch to interface with telephone company data bases for implementing

"number services", such as the 800 service.

SSP/800

Service Switching Point 800 service

SSP800

Service Switching Point 800 service

SSU

Subsequent Signal Unit

ST

STart (pulse)

End Of Dialing Sequence

ST

Start Time

ST7

Channel group type that handles CCSLK terminations.

STAR

Simultaneous Trunk conversion via Automatic Recent change

STAT

STATus

STBY

STandBY

STE

SONET terminating equipment

STF

Some Tests Failed

STLWS

Supplementary Trunk and Line Work Station

STP

Signal Transfer Point

This is a general purpose high-capacity packet switch that performs signaling and message switching and CCS network management functions. The STP routes signaling messages to and from network control points/service control points (NCP/SCP), action points/service switching points (ACP/SSP) and to other STPs. This is the point where the CNI/PSU accesses the CCS network.

ST PH

Signal Transfer Protocol Handler

STPI

Signal Transfer Point International

STS

Synchronous Transport Signal

STSX-1

Synchronous Transport Signal - level 1

SU

Signaling Unit

SUM

SUMmary

SUS

SUSpend message

SW

SoftWare

SYNC

SYNChronous

T&A

Toll And Assistance

TASI

Time Assignment Speech Interpolation

TASI is a technique used to route more than one conversation over a trunk group at a time. This technique may enable 20 phone calls to be routed over 15 circuits.

TAT

Terminating Access Tandem

TAT

Terminating Attempt Trigger

TBI

To Be Idled

TC

Transaction Capabilities

TCA

Transfer Cluster Allowed

TCAP

Transaction Capabilities Application Part

This is a signaling feature that serves as an interface between the number services features and the signaling connection control part (SCCP) of signaling system number 7 (SS7).

TCC

Trunk Class Code

TCIC

Trunk Circuit Identification Code

TCP

Transfer Cluster Prohibited

TCR

Transfer Cluster Restricted

TCRA

Toll Call Record Assembler

TCS

Terminating Code Screening

TE

Threshold Exceeded

Telco

Telephone Company

TEN

Trunk Equipment Number

TEO

Terminating End Office

The terminating end-office is the office which has the terminating line attached to it.

TFC

TransFer Control

TFP

TransFer Prohibited message

TFR

TransFer Restricted message

TG

Trunk Group

TGN

Trunk Group Number

TGSL

Trunk Group Selection Lists

TIC

Translation Integrity Check

TID

Transaction IDentification

TIE

Time Interval Error

TIRKS

Trunks Integrated Records Keeping System

TLWS

Trunk and Line Work Station

TMUX

Transmission Multiplexer

TN

Telephone Number

TN

Transit Network

TNN

Trunk Network Number

TNS

Transit Network Selection

TO

Tandem Office

TO

Toll Office

TOBI

TIRKS Office data administration batch interface

TPC

Translation Point Code

TQ

Trunk Query

TR

Technical Reference

TRA

Traffic Restart Allowed message

TRFC30

30-minute Traffic Report

TRK

TRunK

TRM

Two-mile optically-integrated Remote switching Module

Trunk

The facility between two different entities (that is, central offices, sections of the same switching system) that is used for transmission and/or signaling.

TRW

Traffic Restart Waiting message

TSBI

Trunk State Block Index

TSG

Trunk Sub-Group

TSI

TimeSlot Interchange unit

TSIG

Trunk SIGnaling status indicator

TSP

Translation Signaling Point

TSPS

Traffic Service Position System

TST

Test

TT

Touch-Tone

TT

Translation Type

TTF

Trunk Test Function

TTL

Transistor-Transistor Logic

A common semiconductor technology for building discrete digital logic integrated circuits, typically consisting of two voltage levels: 0 V and +5 V.

TTP

Terminating Terminal Process

The TTP works with the OTP to handle call processing.

TTY

TeleTYpewriter

TU

Trunk Unit

TUCHBD

Trunk Unit CHannel BoarD

UAV

UnAVailable

UBA

UnBlocking Acknowledgment message

UBL

UnBLocking message

UCB

Unit Control Block

This is a data block in the CNI equipment configuration data base.

UCIC

Unequipped Circuit Identification Code

UCL

UnConditional

This is a term used with restoration messages to designate that the ring was restored after a temporary failure without a complete diagnostic process.

UCT

Utility Call Trace

UDS

Unit Data Service

UDTS

Unit DaTa Service

UNEQ

UNEQuipped

UNKN

UNKNown

UNTS

UNTeSteD

UPU

User Part Unavailable

USBL

USaBLLe

USI

User Service Information

UUI

User-to-User Information

VCA

Vacant Code Announcement

This is an announcement provided when a vacant number is dialed.

VCDX

Very Compact Digital Exchange

VLN

Virtual Link Number

VLSI

Very Large Scale Integration

A term describing semiconductor integrated circuits composed of hundreds of thousands of logic elements or memory cells.

VM

Voice Message

VMS

Voice Message Service

VMSR

Voice Message Storage and Retrieval

VPA

Voice Path Assurance

VT1.5

Virtual Tributary 1.5

This involves hardware in the local digital service unit (LDSU) equipped in each switching module that is involved in CCS call processing.

VT1FAC

Virtual Tributary 1.5 Facility

Wink

A brief "off-hook" signal sent from a telephone office to a distant office to indicate that the office is ready to receive the called party telephone number and supervisory information from the distant office.

ZMMPR

15-minute Machine Resource Performance Report

List of Figures

- Figure 2-1 : A Typical CCS Network Configuration
- Figure 2-2 : Relationship Between the CCS Network and the Voice/Data Network
- Figure 2-3 : Lucent Technologies Products STP Simplified Diagram
- Figure 2-4 : CCS Signaling Link
- Figure 2-5 : SS7 Message Format
- Figure 3-1 : 5ESS®-2000 Switch CNI Configuration
- Figure 3.2-1 : IRN2 Ring Cabinet Power - Four Node Arrangement
- Figure 3.2-2 : IRN2 Ring Cabinet Power For More Than Four Nodes
- Figure 3.2-3 : DSU Front Panel
- Figure 3.2-4 : EIA 449 Data Interface Timing Diagram
- Figure 3.2-5 : TTL Data Interface Timing Diagram
- Figure 3.2-6 : LL Test
- Figure 3.2-7 : LL with TP Test
- Figure 3.2-8 : DL Test
- Figure 3.2-9 : RL Test
- Figure 3.2-10 : RL with TP Test
- Figure 3.2-11 : TP Test
- Figure 3.2-12 : Remote Digital Loopback
- Figure 3.2-13 : CSU Loopback
- Figure 3.2-14 : DSU Loopback
- Figure 3.3-1 : UCB Linkage (3B20D)
- Figure 3.3-2 : IUN Complex (3B20D)
- Figure 3.3-3 : UCB Linkage (3B21D)
- Figure 3.3-4 : IUN Complex (3B21D)
- Figure 3.3-5 : Example Page 118 Display - CNI Ring Status
- Figure 3.3-6 : Example Page 1520 Display - Ring Node Status
- Figure 3.3-7 : Example Page 1521 Display - Signaling Link Summary Group
- Figure 3.3-8 : Example Page 1522 Display - Signaling Link Group

Figure 3.3-9 : Example Page 1523 Display - Local Subsystem Status

Figure 3.6-1 : Processor Recovery Message Format

Figure 3.9-1 : Global Title Routing for SSP800, LASS, Line Interface Data Bus (LIDB), and ISUP

Figure 3.9-2 : Query to CCS Network (Global Title STP)

Figure 3.9-3 : STP Message to Data Base (After Global Title Translation)

Figure 3.9-4 : Data Base Reply Message

Figure 3.9-5 : Noncapability Code Routing Configuration

Figure 3.9-6 : Capability Code Routing Configuration

Figure 3.10-1 : E-Link and A-Link Set Routing

Figure 3.11-1 : SS7 Signaling Connections

Figure 3.18-1 : IRN2 CNI Ring

Figure 4-1 : Digital Signaling Link Block Diagram

Figure 4-2 : Digital Signaling Links

Figure 5.2-1 : SS7 ISUP Call Processing Message Flow

Figure 5.2-2 : Delay in Interworking or Alerting a Terminating Party with VPA

Figure 5.2-3 : Delay in Termination of Call - Non-ISDN Called Party Disconnects

Figure 5.3-1 : 5E6 Call Setup Failure

Figure 5.3-2 : Call Setup Failure

Figure 5.8-1 : Trunk Blocking Sequence

Figure 5.8-2 : Trunk Unblocking Sequence

Figure 5.8-3 : Continuity Recheck Sequence

Figure 6-1 : SS7 Configuration

Figure 6-2 : New Point Code

Figure 6-3 : Flash Cut of Lines

Figure 6-4 : SS7 Trunk Testing Configuration

Figure 6-5 : Link Testing Procedures

Figure 6-6 : Link Testing Messages

Figure 6-7 : VPA Test Exchanges

Figure 7-1 : STAR Hardware Configuration

Figure 7-2 : Enhanced STAR Call Data Flow Diagram

Figure 8.3-1 : OP:Ring Commands

Figure 8.3-2 : IRN2 CNI Shelves Circuit Pack Arrangement

Figure 8.5-1 : Checking the Ring Capacity Against HV Values

Figure 8.7-1 : CNI Problem Indicators

Figure 9.2-1 : Processing of a Q.931/ISUP Call Through the 5ESS®-2000 Switch

Figure 9.2-2 : ISDN/ISUP Message Flow Originating End

Figure 9.2-3 : ISDN/ISUP Message Flow Terminating End

Figure 9.2-4 : Call Failure Message Flow ISDN/ISUP

Figure 9.2-5 : Call Failure Message Flow ISDN/ISUP Announcements

Figure 9.4-1 : ISDN/ISUP Fast Connect Message Flow - Originating End - 5E6

Figure 9.4-2 : ISDN/ISUP Fast Connect Message Flow - Originating End

Figure 9.4-3 : ISDN/ISUP Fast Connect Message Flow - Terminating End - 5E6

Figure 9.4-4 : ISDN/ISUP Fast Connect Message Flow - Terminating End

Figure 9.4-5 : OEO PRI Calling Line Identification Logic

Figure 9.4-6 : OEO BRI Calling Line Identification Logic

Figure 10-1 : Network Interconnect Architecture

Figure 10-2 : ISUP Network Interconnect - End Office to Toll Direct

Figure 10-3 : ISUP Network Interconnect Call - via Access Tandem

Figure 10-4 : Interworking - Equal Access End Office to Inter-LATA Carrier

Figure 10-5 : Interworking - Equal Access End Office to International Carrier

Figure 10-6 : Interworking - Traditional Inband Signaling End Office to Inter-LATA Carrier

Figure 10-7 : Interworking - Traditional Inband Signaling End Office to International Carrier

Figure 10-8 : Interworking ISUP to Equal Access Inband Signaling - Inter-LATA Carrier

Figure 10-9 : Interworking ISUP to Equal Access Inband Signaling - International Carrier

Figure 10-10 : Interworking ISUP Signaling to Traditional Inband

Figure 10-11 : 950 + Call to Feature Group B Carrier via Traditional Signaling

Figure 10-12 : 950 + Call to Equal Access Plan Carrier via Equal Access Signaling

Figure 10-13 : Interworking - FGB Inband NC End Office to Inter-LATA or International Carrier

Figure 10-14 : ISUP Signaling to Feature Group B Inband Signaling

Figure 10-15 : CIP With Inband Signaling Between An End Office And Access Tandem

Figure 10-16 : Call Setup ISUP to Inband Signaling

Figure 10-17 : 5E6 Software Release Positions for Recoding Cause Location Values

Figure 10-18 : 5E7 Software Release Positions for Recoding Cause Location Values

Figure 11.1-1 : Module Compatibility for IMTs

Figure 11.1-2 : Basic IMT Configuration

Figure 11.1-3 : IMT Configuration Using Tandem Routing

Figure 11.1-4 : IMT Configuration Using Overflow Tandem Routing

Figure 11.1-5 : IMT Configuration Using Two Types of Signaling

Figure 11.2-1 : VCDX Loop-around Intramodule Trunk

Figure 11.3-1 : ISUP Intramodule Loop-around Trunk

Figure 11.8-1 : Equal Access Signaling Sequence

Figure 11.8-2 : Traditional Signaling Sequence

Figure 11.8-3 : CAMA Signaling Sequence

Figure 11.10-1 : TCAP Message Flow for Terminating Scanning

Figure 11.10-2 : TCAP Message Flow for Originating Scanning

Figure 11.12-1 : N x DS0 Call Origination/Termination Scenario

Figure 11.14-1 : ISVM Switch Interface Configurations and Required Software Releases

Figure 11.15-1 : AMPS Overview

Figure 11.15-2 : Switch AMPS Interworking to ISUP7 Originating Switch DCS Office

Figure 11.15-3 : Switch AMPS Interworking to ISUP7 Terminating Switch DCS Office

Figure 12.1-1 : Typical VCDX CCS Network Configuration 5E11 Software Release

Figure 12.1-2 : Typical GSM CCS Network Configuration 5E12 Software Release

Figure 12.1-3 : GSM Signaling Link Architecture (SM)

Figure 12.1-4 : GSM Signaling Link Architecture (SM-2000)

Figure 12.5-1 : Typical SP Routing Paths

Figure 12.5-2 : Typical *MRVT* Message Flow

Figure 12.5-3 : Typical *MRVA* Message Flow

Figure 12.5-4 : *MRVT/ MRVA* Message Flow at an STP

Figure 12.5-5 : MRVT Example 1

Figure 12.5-6 : MRVT Example 2 Routes

Figure 12.5-7 : MRVT Example 2 Message Flow

Figure 12.5-8 : MRVT Example 3 Message Flow

Figure 12.5-9 : MRVT Example 4 Message Flow

Figure 12.5-10 : MRVT Example 5

Figure 12.5-11 : MRVT Example 6

Figure 12.5-12 : Typical SRVT Message Flow

Figure 12.5-13 : Typical SRVA Message Flow

Figure 12.5-14 : SRVT/ SRVA Message Flow at a TSP

Figure 12.5-15 : SRVT Example 1

Figure 12.5-16 : SRVT Example 2

Figure 12.5-17 : SRVT Example 3

Figure 12.5-18 : SRVT Example 4

Figure 12.5-19 : SRVT Example 5

Figure 12.5-20 : SRVT Example 6

Figure 12.5-21 : SRVT Example 7

Figure 12.5-22 : SRVT Example 8

List of Tables

Table 2-1 : SS7 Protocol Description

Table 3.1-1 : Environmental Limits

Table 3.2-1 : IRN2 Components

Table 3.2-2 : IRN2 Ring Cabinet Power For Four Node Arrangement - Required Facility Assignment

Table 3.2-3 : IRN2 Ring Cabinet Power For More Than Four Nodes - Required Facility Assignment

Table 3.3-1 : Administrative Module Functions

Table 3.3-2 : Node Processor Functions

Table 3.3-3 : IRN2 CNI Node UCB Population Aid

Table 3.3-4 : IRN2 UCB Field 25 Hardware Version (HV) Values

Table 3.6-1 : PRM Digits 14 and 15 CNIINIT's Child Process Creation

Table 3.6-2 : PRM Digits 14 and 15 CNIINIT's Default Audit

Table 3.10-1 : Recent Change Views Impacted By E-LINK

Table 3.11-1 : Recent Change Views Impacted By F-Link

Table 3.12-1 : Recent Change Views Impacted By FPCR

Table 3.13.1-1 : IMS Measurement Descriptions

Table 3.13.1-2 : SS7 CNI Measurement Descriptions

Table 3.14-1 : Office Dependent User Changeable Parameters

Table 3.14-2 : Linkset Dependent User Changeable Parameters

Table 3.15-1 : Recent Change View Numbers

Table 3.19-1 : Signaling End Point (SEP) Timers

Table 4-1 : Signaling Link State Transitions

Table 5.1-1 : ISUP Messages And Parameters

Table 5.1-2 : ISUP Messages Priority

Table 5.3-1 : Call Failure Treatment For Non-ISDN Originated Calls

Table 5.3-2 : Release Message Cause Coding For Call Failure

Table 5.3-3 : Tone and Announcement From Cause Coding

Table 5.3-4 : Unsupported Call Release Causes

Table 5.3-5 : OEO Backward CPG Received (With Cut-Through Indication)

Table 5.3-6 : OEO Backward CPG Received (Without Cut-Through Indication)

Table 5.3-7 : OEO Forward CPG Sent (Cut-Through Indication Not Valid)

Table 5.3-8 : Tandem Backward CPG Received (With Cut-Through Indication)

Table 5.3-9 : Tandem Backward CPG Received (Without Cut-Through Indication)

Table 5.3-10 : Tandem Forward CPG Received (Cut-Through Indication Not Valid)

Table 5.3-11 : TEO Backward CPG Sent (With Cut-Through Indication)

Table 5.3-12 : TEO Backward CPG Generated (Without Cut-Through Indication)

Table 5.3-13 : TEO Forward CPG Received (Cut-Through Indication not Valid)

Table 5.5-1 : Recent Change Views

Table 5.5-2 : OP:SS7 Message Information

Table 5.6-1 : Support Systems Interfaces

Table 5.6-2 : Timers

Table 5.8-1 : ISUP Specific MDIIs

Table 5.8-2 : Locally Blocked Status to Blocking Message Mapping

Table 5.8-3 : Locally Blocked Status Deletion to Unblocking Message Mapping

Table 5.8-4 : MDII Messages Printed When Acknowledgement Message Not Received

Table 5.8-5 : Query Statuses

Table 5.8-6 : Transient and Unequipped State Corrections

Table 5.8-7 : Maintenance State Corrections

Table 5.8-8 : Call Processing State Corrections

Table 5.8-9 : Data Transmitted in a CVR

Table 5.8-10 : Supported ISUP Trunk Test Calls

Table 5.8-11 : Trunk and Line Work Station Features

Table 5.9-1 : VPA Loss Threshold Level

Table 5.9-2 : VPA Hardware Threshold Level

Table 5.9-3 : VPA Loss Level: 4-Wire

Table 5.9-4 : VPA Loss Level: 2-Wire

Table 5.9-5 : VPA Frequencies Used For Each VPA Type

Table 7-1 : Example Manual Trunk Conversion Planning Data

Table 8.3-1 : CNI Diagnostic Message Input Variations

Table 8.3-2 : Input (OP) Messages for Obtaining CNI Ring Status

Table 8.3-3 : Major Node State Abbreviations

Table 8.3-4 : IRN2 Ring Peripheral Controller Node Diagnostic Phases

Table 8.3-5 : IRN2 IMS User Node Diagnostic Phases

Table 8.3-6 : IRN2 Direct Link Node Diagnostic Phases

Table 8.3-7 : IRN2 Link Node Diagnostic Phases

Table 8.3-8 : IRN2 Ring Peripheral Controller Node Trouble Location Circuit Pack List

Table 8.3-9 : IRN2 Link Node Trouble Location Circuit Pack List

Table 8.3-10 : IRN2 Direct Link Node 30 (DLN30) Trouble Location Circuit Pack List

Table 8.4-1 : CNI/IMS Trouble Indicators and Analysis MROP Output Messages

Table 8.4-2 : CNI/IMS Trouble Indicators and Analysis Visual Alarms At Maintenance CRT

Table 8.4-3 : CNI/IMS Trouble Indicators and Analysis Visual Alarms At Ring Node Cabinet

Table 8.4-4 : CNI/IMS Trouble Indicators and Analysis Audible Alarms

Table 8.5-1 : Manual Diagnostics and Restoral Requests

Table 8.5-2 : LED Illumination for Circuit Pack Removal

Table 8.7-1 : 118 Page Status Indicators

Table 8.7-2 : 118 Page Status Indicators — Node State

Table 8.7-3 : 118 Page Status Indicators — Signaling Link

Table 9.2-1 : Message Mapping From ISDN User Protocol To ISUP Protocol

Table 9.2-2 : Message Mapping from ISUP Protocol To ISDN User Protocol

Table 9.2-3 : Mapping of Q.931 REL, REL COMP, or DISC to an ISUP ACM, CPG, or REL

Table 9.2-4 : Mapping of ISUP REL to Q.931 REL, REL COMP, or DISC

Table 9.2-5 : Mapping of Q.931 CONNect to ISUP ANM

Table 9.2-6 : Mapping of ISUP ANM to Q.931 CONNECT

Table 9.2-7 : Mapping of Q.931 ALERTing to ISUP ACM or CPG

Table 9.2-8 : Mapping of ISUP ACM or CPG to Q.931 ALERTING

Table 9.2-9 : Mapping of Q.931 PROGRESS to ISUP ACM or CPG

Table 9.2-10 : Mapping of ISUP ACM or CPG to Q.931 PROGRESS

Table 9.2-11 : Mapping of Q.931 SETUP to ISUP IAM

Table 9.2-12 : Mapping of ISUP IAM to Q.931 SETUP

Table 9.3-1 : MA-UUI Information Element Summary

Table 9.4-1 : Call Present State

Table 9.4-2 : Incoming Call Proceeding State

Table 9.4-3 : Delay State

Table 9.4-4 : Delayed Call Proceeding State

Table 9.4-5 : Local Exchange Modification

Table 9.4-6 : Coding of SS7 Cause Indicators Parameter

Table 9.5-1 : ACD Call Present State

Table 9.5-2 : ACD Incoming Call Proceeding State

Table 9.5-3 : ACD Delay State

Table 9.5-4 : ACD Delayed Call Proceeding State

Table 10-1 : CSI Parameter Coding

Table 10-2 : Called Party Number (CPN) and Transit Network Selection (TNS) Parameters Coding

Table 10-3 : Originating Line Information (I and II Digits)

Table 10-4 : Inter-LATA Signaling

Table 10-5 : International Carrier Signaling

Table 10-6 : Values Used In Any Carrier Identification Parameter

Table 10-7 : Table 60 to ANI/CPN Indicator

Table 10-8 : Access Recording

Table 10-9 : Egress Recording

Table 10-10 : Office Data Summary

Table 11.1-1 : Module Compatibility

Table 11.1-2 : Primary IMT Provisioning

Table 11.1-3 : Emergency IMT Provisioning

Table 11.1-4 : Destination Point Code

Table 11.6-1 : 30-Minute Traffic Report: ISUP Utilization

Table 11.6-2 : 30-Minute Report: ISUP Performance

Table 11.6-3 : 30-Minute Traffic Report: ISUP Circuit Availability

Table 11.6-4 : 30-Minute Traffic Report: ISUP End-to-End Connection Performance

Table 11.8-1 : Traditional Signaling "II" Code Meanings
Table 11.8-2 : Mapping Conversion of "I" Codes to "II" Codes
Table 11.8-3 : Call Codes for Number Service Billing
Table 11.8-4 : Trapping SSP Events
Table 11.9-1 : SSP800 AMA Records Impacted By The SSP800/ASP Feature
Table 11.10-1 : Expected DN-Match and Line Type Values
Table 11.13-1 : OSPS Use of Common Channel Signaling
Table 11.13-2 : Calling Card Recognition/Attributes - Recent Change Views
Table 11.13-3 : LEC Calling Card Service Validation - Recent Change Views
Table 11.13-4 : Billing Number Screening Queries Validation: Recent Change Views
Table 11.13-5 : Changing Query Time-Out Values: Recent Change Views
Table 11.13-6 : Linear Cutback Control Duration: Recent Change Views
Table 11.13-7 : Test Queries Input/Output Messages
Table 11.13-8 : Event Trapping Input/Output Messages
Table 11.13-9 : Alarm Threshold Report: Recent Change View
Table 11.15-1 : 5ESS®-2000 Switch DCS Ignored Items
Table 11.15-2 : Mapping From ECPC To ISUP Signals
Table 11.15-3 : Mapping From ISUP Signal To ECPC Message
Table 12.2-1 : CCSLK States in a GSM
Table 12.2-2 : SDL States in a GSM
Table 12.2-3 : Summary LS States in a GSM
Table 12.2-4 : Intra-SM MD Link States
Table 12.2-5 : 1533 MCC Page CCSLK Reconfiguration Menu Commands
Table 12.5-1 : MRVT Error Codes
Table 12.5-2 : Supplemental MRVR Error Information
Table 12.5-3 : SRVR Error Codes
Table 12.5-4 : Supplemental SRVR Error Information
Table 13.1-1 : GSM Signaling RC/V Views
Table 13.1-2 : SM/SM-2000 to GSM Conversion

Table 13.1-3 : On-going GSM SS7 Provisioning Activities
Table 13.1-4 : Removal of CCS Capabilities from a GSM
Table 13.1.2-1 : MTP Level 2 Timer Range
Table 13.1.3-1 : Pre-5E13 MTP Level 3 Timer Ranges
Table 13.1.3-2 : 5E13 and Later MTP Level 3 Timer Ranges
Table 13.1.22-1 : OMAP Timer/Parameter Ranges
Table 13.2-1 : ISUP Trunking RC/V Views
Table 13.2-2 : Install Trunk Routes from a GSM
Table 13.2-3 : Typical ISUP Trunk Provisioning Activities
Table 13.2-4 : Deleting All ISUP Trunk Routes on a GSM
Table 13.2-5 : Converting Existing Trunks to GSM Signaling Platform
Table 13.3-1 : GSM SCCP RC/V Views
Table 13.3-2 : SCCP Growth Procedures
Table 13.3-3 : SCCP Updating Procedures
Table 13.3-4 : SCCP Deletion Procedures
Table 13.4-1 : MTP/SCCP Measurements Collection RC/V Views
Table 13.4-2 : Define MTP/SCCP Measurement Collection on GSMs
Table 13.5-1 : TCAP Signaling Platform Definition RC/V Views
Table 13.5-2 : Designate Signaling Platform for TCAP Applications
Table 13.5-3 : TCAP Application Availability