Lucent Technologies
Bell Labs Innovations

Signaling System 7
LEC Network

Operations, Administration, and Maintenance

256-015-300
Issue 3
October 1996

Notice

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

Trademarks

Ordering Information

To order additional copies of this document, 256-015-300, contact:

Lucent Technologies Customer Information Center (CIC)
P.O. Box 19901
Indianapolis, IN 46219

Phone: 1-888-582-3688

Support Telephone Number

Lucent Technologies provides a telephone number for you to use to report errors or to ask questions about the information in this document. The support telephone number is 1-800-334-0404 (within North Carolina dial 1-910-727-6681).

Developed by Lucent Technologies Network Systems Customer Training and Information Products.

How Are We Doing?

Document Title: Signaling System 7 LEC Network Operations, Administration, and Maintenance

Document No.: 256-015-300 Issue 3 Date: October 1996

Lucent Technologies welcomes your feedback on this document. Your comments can be of great value in helping us improve our documentation.

1. Please rate the effectiveness of this document in the following areas:

	Excellent	Good	Fair	Poor	Not Applicable
Ease of Use					////////////////////
Clarity					////////////////////
Completeness					////////////////////
Accuracy					////////////////////
Organization					////////////////////
Appearance					////////////////////
Examples					
Illustrations					
Overall Satisfaction					////////////////////

2. Please check the ways you feel we could improve this document:

- ☐ Improve the overview/introduction
- ☐ Improve the table of contents
- ☐ Improve the organization
- ☐ Include more figures
- ☐ Add more examples
- ☐ Add more detail
- ☐ Make it more concise/brief
- ☐ Add more step-by-step procedures/tutorials
- ☐ Add more troubleshooting information
- ☐ Make it less technical
- ☐ Add more/better quick reference aids
- ☐ Improve the index

Please provide details for the suggested improvement. _____

_____

3. What did you like most about this document?

_____

_____

4. Feel free to write any comments below or on an attached sheet.

_____

_____

_____

_____

If we may contact you concerning your comments, please complete the following:

Name: _____ Telephone Number: _____

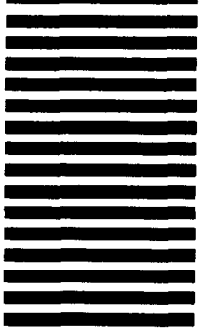
Company/Organization: _____ Date: _____

Address: _____

When you have completed this form, please fold, tape, and return to address on back or Fax to: 910-727-3043.

Do Not Cut—Fold Here And Tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES



Lucent Technologies
Bell Labs Innovations

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 1999 GREENSBORO, N.C.

POSTAGE WILL BE PAID BY ADDRESSEE

DOCUMENTATION SERVICES
2400 Reynolda Road
Winston-Salem, NC 27199-2029

Contents Page

Contents Page

Contents Page

Contents Page

Figures

Contents Page

Contents Page

Contents Page

Contents Page

Tables

Contents Page

Contents Page

Contents Page

Contents Page

Contents Page

About This Document

1

Contents Page

About This Document

1

1. Purpose

1.01 This document describes Common Network Interface, Central Office, Lucent Technologies *A-I-Net*® advanced intelligent network products Signal Transfer Point (STP) and Service Control Point (SCP) interactions within a Local Exchange Carrier (LEC*) network. It also describes the associated data which must be consistent within the LEC network. This is necessary for Local Access and Transport Area (LATA) Signaling System 7 (SS7) services to function correctly.

2. Scope

2.01 This document is designed to address interconnection and interaction of Lucent Technologies SS7 products. The information should assist administrators of a LEC network in engineering certain entities across network elements. Included are considerations pertinent to Integrated Services Digital Network—User Part (ISDN-UP)†, Local Area Signaling Service (LASS), Service Switching Point (SSP), Advanced Services Platform (ASP), Network Interconnect (NI), and other features that use SS7 capabilities. This document also provides Operational, Troubleshooting, and Maintenance procedures.

---

* In this document, the term LECs includes Regional Bell Operating Companies as well as independent carriers of local telephone companies.

† ISDN-UP is frequently referred to as Integrated Service Digital Network—User Part (ISUP). ISUP is used throughout this document to refer to ISDN-UP trunk signaling protocol and the associated switch capabilities.

While the information in this document refers only to Lucent Technologies products, the requirements for OA&M activities between switches and STPs generally apply for non-Lucent Technologies products.

NOTE:
If an item applies only to a Lucent Technologies STP, the text references "*A-I-Net* products STP" rather than "STP." If it applies only to a Lucent Technologies switching product, the text references the particular switch involved.

Reason for Reissue

2.02 Issue 3 of this document includes the addition of several new generic software releases.

The major changes are:

(a) "STP Gateway Screening" information references in Chapter 3 have been updated to *A-I-Net*® products STP Release 2 documents.

(b) The modification or addition of generic software 1AE12, 4E18, 5E9, and *A-I-Net* products STP Release 2 data requirements, assignments, and consistency rules for the SS7 network throughout the document and particularly in Chapter 3, "Data Administration Guidelines."

(c) Small Network Specific Requirements scenarios have been updated in Chapter 3, "Data Administration Guidelines."

(d) Figure 3-1 has been updated to include E-link configuration.

(e) In Table 3-C, Office C point codes have been corrected and *A-I-Net* products STP 2 and 3 point codes have been added.

(f) In Figure 3-2, link set data has been updated to include E-link data and to match Figure 3-1.

(g) Figure 3-4 has been changed to reflect 1AP3F, 5E9.2, and 4AP12 [with Alternate A-Link Set Routing (ALSR)] for switch cluster data.

(h) Additional protocol timer and parameter settings which are now recent changeable in 5E9, 1AP3F, and 4AP12 have been added to Chapter 3, Part 7. New Tables 3-H and 3-I have also been added.

(i) Chapter 3, Part 8 now contains Extended Access Link (E-Link)/Alternate A-Link Set Routing. Paragraphs 12.08 through 12.15, Tone and Announcement Treatment, 4E14 and 4E15 treatment, have been removed and replaced.

(j) NI Data Audit 10 has been added to Chapter 4, Part 7. Table 4-AG has been updated.

(k) Figure 6-2 has been changed to include 1AP3E, 5E7, and 4AP10.

(l) Figure 6-2 has been added to include 1AP3F, 4AP12, and 5E9. Figure 6-3 has been added to include *A-I-Net* products STP, RLS 2.

(m) Figure 6-30, "IAM Message Format", has been updated.

(n) Chapter 7, Part 2, "Signaling Link Rehome Procedure", has been corrected, and OPC7NET messages have been updated.

(o) All references to Bellcore and Lucent documentation and products have been corrected or updated throughout the document.

2.03 The intent of this document is to provide a network viewpoint of Operational, Administrative, and Maintenance (OA&M) guidelines, procedures and data that directly impact the functionality of a LEC SS7 network. While a number of documents exist that discuss this information, most are system-specific in their content.

2.04 This document attempts to minimize duplication and thus references Lucent Technologies system-specific documentation (that is, 1A ESS™ switch, 4ESS™ switch, 5ESS® switch, or *A-I-Net* products STP) when appropriate. It does not describe how to configure a LEC SS7 network, but is meant to provide useful guidelines and procedures used in managing and engineering LEC SS7 network elements.

2.05 The 5ESS-2000 switch Compact Digital Exchange (CDX) is a compact version of the 5ESS switch. The SS7 capabilities for the 5ESS-2000 switch CDX are provided by the standard 5ESS switch hardware and software. For this document, all the sections that pertain to the 5ESS switch will also pertain to the 5ESS-2000 switch CDX and will not be identified separately.

3. Document Organization

3.01 The remaining chapters and are described as follows:

(a) Chapter 2—Describes network-level operational procedures and guidelines.

(b) Chapter 3—Describes the network-level administrative guidelines, including the data that must be populated for ISUP functionality within the LEC network. This chapter also provides the ISUP data and data consistency requirements for call processing and trunk maintenance capabilities. In addition, this chapter describes Internetwork, Advanced Services Platform (ASP), Small Network, Connectionless Services, LASS, and SSP requirement data.

(c) Chapter 4—Describes network-level maintenance procedures and guidelines.

(d) Chapter 5—Identifies network measurements.

(e) Chapter 6— Describes tools for verifying the accuracy of Common Network Interface, Lucent Technologies switch, and *A-I-Net* products STP data.

(f) Chapter 7—Addresses some miscellaneous engineering considerations that could not easily fit into Chapters 2 through 6.

(g) Chapter 8—Provides a list of acronyms used in this document.

(h) Index — List relevant topics and where they can be found in this document.

4. Document Maintenance

4.01 As enhancements and additions are made to SS7 capabilities, this document will be updated and reissued to communicate affecting changes in Lucent Technologies switch and *A-I-Net* products STP OA&M guidelines and procedures.

5. Network Impact

5.01 Procedures and guidelines mentioned in this document may have an impact on the local switch, *A-I-Net* products STP, or other network elements (that is, connecting the switch, STP, and other network elements). Where applicable, key considerations are denoted by a NOTE (pencil head) or a CAUTION (triangle).

5.02 This document is not meant to replace system-specific OA&M documentation, but rather to enhance its content with a network perspective.

6. Customer Satisfaction and Complaint Reporting

6.01 As a valued customer, we appreciate and act on any comments, complaints, or suggestions you may have about this document and our product. The Network Services Customer Support group makes every effort to provide quality, error-free documentation. Our goal is to achieve a high degree of satisfaction from our document users. In order to continue to provide this quality and satisfaction, we are requesting your assistance and are providing the tools/procedures to make your contribution as painless as possible.

Form, Format, and Printing Complaints

6.02 If there are complaints or suggestions for improvement of the form, format, or print quality of this document, please fill out the form ("How Are We Doing") accompanying this document and mail or Fax it as directed on the form.

Technical Content Complaints/Suggestions

6.03 If you have complaints or suggestions concerning the technical content of this document, please call the Customer Technical Assistance Management (CTAM)

Hotline on 1-800-225-4672 and ask for the "Network Editor." A trouble ticket will be opened, your inquiry will be recorded, and a Network Customer Advocate will be assigned to resolve the problem. You will be advised of the status and resolution of your inquiry before the ticket is closed.

Operational Procedures and Guidelines

2

Contents Page

Contents Page

Operational Procedures and Guidelines

2

1. Overview of ISUP Call Processing

1.01 With its protocol structure, signaling routing mechanisms, variable message lengths, and higher data transfer rate, Integrated Services Digital Network—User Part (ISUP) signaling offers many advantages over Per-Trunk Signaling (PTS). Examples of PTS are Multifrequency (MF) and Dial Pulse (DP) signaling. However, it is important to note that the improvements are related primarily to *signaling and services.* Plain Old Telephone Service (POTS) call processing functions (for example, address analysis, screening, routing, trunk selection, digit conversion, and alerting) are the same as those used in PTS. Calls are still routed in stages as shown in Figure 2-1.

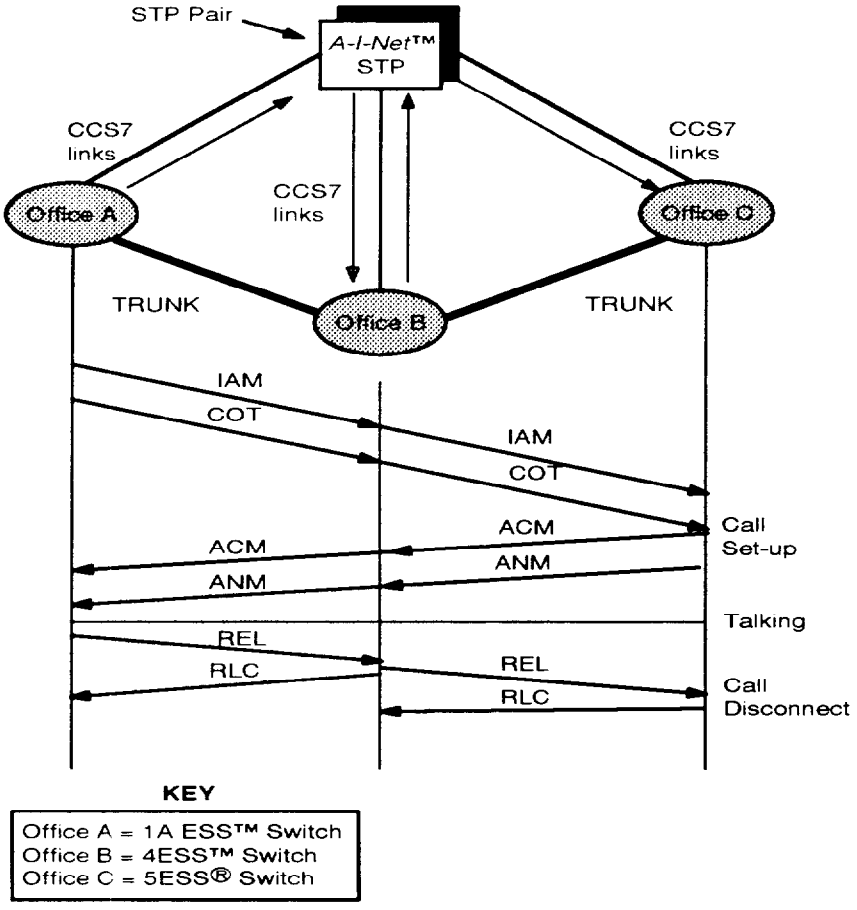


Figure 2-1. ISUP Call Processing in the SS7 Network

1.02 For the following description, refer to Figure 2-1. Assume a basic interoffice voice call, originating from Office **A** and terminating at Office **C** (via Tandem Office **B**), is to be made. Notice that with ISUP signaling, all signaling messages are relayed through one or more Signaling Transfer Points (STPs).

1.03 After Office **A** receives the called number from the originating party, routing for the call is determined using internal translations (as in PTS). An Initial Address Message (IAM) containing the routing digits (plus additional data) is then sent via one of the STPs to Tandem Office **B** for a selected ISUP circuit. This circuit is uniquely identified by a Trunk Circuit Identification Code (TCIC), and the Point Codes of Offices **A** and **B**. All ISUP messages include a TCIC identifying the related circuit/trunk.

1.04 Since ISUP does not signal through the actual speech path, it is necessary to ensure that acceptable transmission can occur. A voice continuity, or Voice Path Assurance (VPA), test can be requested in the IAM on the outgoing circuit. Results of the test (success or failure) are sent by originating Office **A** in a Continuity message (COT) to Tandem Office **B***.

1.05 On receipt of the IAM, Office **B** handles the VPA request and then examines the called party address. Digit deletion/prefixing and routing are again determined using internal translations. Office **B** then formats an IAM for a selected ISUP outgoing circuit and sends the message via an STP to terminating Office **C**†. The IAM contains the TCIC associated with the outgoing circuit. Finally, regardless of whether or not Office **A** requested a VPA test on the incoming circuit, Office **B** may request a VPA test on the outgoing circuit. The calling party number is available to Office **C** which has an option that allows the number to be displayed. For additional information, refer to Chapter 3, "LASS Specific Requirements."

1.06 An Address Complete Message (ACM) is sent by Office **C** to Office **B** acknowledging that the address information has been received at the terminating end office and that no tandeming occurs. At this point, Office **C** provides audible ringing on the incoming trunk and rings the terminating line. Meanwhile, Office **B** immediately passes the ACM to Office **A**, and the interoffice call path is established. An Answer message (ANM) corresponding to the answer used in MF signaling is initiated when the ring trip (off-hook on the terminating line) occurs.

1.07 Assuming the calling party initiates the release procedure (that is, disconnects first), a Release (REL) message is sent from Office **A** to Office **B**. The REL message is then sent to Office **C**. Simultaneously, the switch path from Office **A** to Office **B** is disconnected, and a Release Complete (RLC) message is returned to Office **A**. On receipt of the REL at Office **C**, the switch path from Office **B** to Office **C** is released and an RLC is returned to Office **B**‡.

---

* In this example, the call setup sequence includes a continuity test. Note that the continuity tests can be performed on a sampling basis. For further information, refer to Chapter 3, "Voice Path Assurance Data."

† The intermediate office (in this case **B**) can either send the formatted IAM immediately after the incoming IAM is received, or wait until the incoming continuity check procedure is completed.

‡ A similar procedure is followed if a POTS called party initiates the release. The only difference is that a Suspend (SUS) message is returned all the way from Office C to Office A first. Office A then proceeds as above.

2. Network Management

SS7 Automatic Congestion Control for Integrated Services Digital Network—User Part

A. Definition

2.01 When the circuit network is under stress due to traffic overload or major facility failure(s), network management controls must be initiated at common channel exchanges to maximize the efficiency of the network and to protect its integrity and security.

2.02 Automatic Congestion Control (ACC) is a feature that automatically reduces the Signaling System (SS7) Integrated Services Digital Network—User Part (ISUP) traffic load to a congested switch. This feature determines when an office is in congestion while SS7 is being used between offices. In response to an IAM, a congested office sends a REL or Address Complete Message.

2.03 The SS7 message contains the Automatic Congestion Control Level (ACCL) parameter. The ACCL parameter has three possible values:

Machine Congestion Level 0 (MC0) indicating no congestion

Machine Congestion Level 1 (MC1) indicating minor congestion

Machine Congestion Level 2 (MC2) indicating major congestion

Offices receiving and able to interpret the ACCL parameter should throttle back on calls offered to the congested office.

NOTE:
The 5ESS® and 1A ESS™ switches do not code ACCL with the MC0 value and ignore that value if received. MC3, if received, is treated as an MC2. For additional information, refer to Section E, "Deactivation."

B. Availability

2.04 The ACC feature (Table 2-A) is available in the following switch generic software releases:

Table 2-A. ACC Generic Software Releases

1A ESS™ Switch	4ESS™ Switch	5ESS® Switch
1AE11 and later	4E16 and later	5E6 and later

C. Setup

2.05 To specify the throttling actions in a 1A ESS switch when an ACCL parameter indicating MC1 or MC2 is received, refer to the **RC:TG** recent change message (**CNTRLT** and **RSPCAT** keywords) in 231-318-334, *Trunk Translation Recent Change (RC) Formats*. The percentage of traffic that is affected by network management controls is calculated based on the response category (RSPCAT) and ACC level of congestion indicated in the REL message optional parameter. Table 2-B reflects the calculation.

Table 2-B. Network Management Control Calculation

Switch	Resp. Cat.	AC1 AR	AC1 DR	AC2 AR	AC2 DR	AC1 AR HTR	AC1 DR HTR	AC2 AR HTR	AC2 DR HTR
1A ESS™	0	75*	50*	75*	75*	—	—	—	—
1A ESS	1	0	0	100	0	—	—	—	—
1A ESS	2	0	0	100	75	—	—	—	—
1A ESS	3	100	0	100	75	—	—	—	—
4ESS™	A	0	0	0	0	100	0	100	75
4ESS	B	0	0	100	0	100	0	100	0
4ESS	C	0	0	100	0	100	75	100	75
4ESS	D	100	0	100	100	100	0	100	100
4ESS	E	0	0	0	0	100	75	100	87
4ESS	F	0	0	0	0	0	0	100	0
4ESS	G	0	0	0	0	0	0	100	100
4ESS	H	0	0	0	0	100	0	100	100
4ESS	I	0	0	100	0	100	100	100	100
4ESS	J	0	0	100	75	100	100	100	100
4ESS	K	100	0	100	75	100	100	100	100
4ESS	L	75†	50†	75†	75†	75†	50†	75†	75†
4ESS	M	0	0	0	0	0	0	0	0
4ESS	N	0	0	0	0	0	0	0	0
5ESS®	A	0	0	0	0	—	—	—	—
5ESS	B	0	0	0	0	—	—	—	—
5ESS	C	75‡	50‡	75‡	75‡	—	—	—	—
5ESS	D	0	0	100	0	—	—	—	—
5ESS	E	0	0	100	75	—	—	—	—
5ESS	F	100	0	100	75	—	—	—	—

* In 1AE11.07 and later.

† In 4E16R4 and later.

‡ In 5E8 and later.

AC—Automatic Congestion Level Received

AR—Alternate Routed

DR—Direct Routed

HTR—Hard to Reach

Resp. Cat.—Respond Category

2.06 To specify which offices can send and receive ACC information to the 1A ESS switch, refer to the **RC:POINTC** input message (**PC** and **ACCA** keywords) in 231-318-334, *Trunk Translation Recent Change Formats.* To verify whether or not far-end offices can send ACC information to the 1A ESS switch, refer to the **VF:RUGRAT** input message (**PC** keyword) in the 1A ESS switch *IM-6A001-01* manual and the **VF24** output message in the 1A ESS switch *OM-6A001-01* manual.

2.07 The ACC feature parameters in a 4ESS™ switch can only be entered on a terminal attached to a network management channel. Throttling actions are viewed and specified on the network management CN02 page. The response categories are assigned on a trunk subgroup basis.

2.08 To prevent the 4ESS switch from sending ACCL to switches that are unable to interpret it, use the NM CN03 page. The control of ACCL is done on a trunk subgroup basis.

2.09 To specify the throttling actions in a 5ESS switch when an ACCL parameter indicating MC1 or MC2 is received, refer to the **ASGN:DOC** and **CLR:DOC** input messages in 235-600-700, *5ESS Switch Input Messages* and their corresponding output messages in 235-600-750, *5ESS Switch Output Messages.* To view the current ACC response actions, refer to the **OP:DOC** input and output messages in the same Practices.

NOTE:
The ACCL transmission on a 5ESS switch may be inhibited or activated on an office basis via **INH:DSILC** and **ALW:DSILC**. For additional information, refer to 235-600-700, *5ESS Switch Input Messages Manual* and 235-600-750, *5ESS Switch Output Message Manual.*

D. Activation

2.10 The switch determines if it is congested by an internal dynamic calculation having no user changeable parameters. Another switch (capable of processing the ACCL parameter) reduces traffic to the congested switch when it receives a REL message with an ACCL parameter value of MC1 or MC2. The following messages are reported when a REL message with the ACCL parameter is received (Table 2-C).

Table 2-C. Automatic Congestion Control Level Received

Office Type	ACC Activation Indication
1A ESS™ Switch	When the control is invoked, a TOC02 message prints indicating that control is imposed.
4ESS™ Switch	**REPT: MCa DOC RECEIVED ON THIS TSG: b** where **a** = 0, 1, or 2 for the congestion level and **b** = CIN identifying the trunk subgroup which received the ACCL.
5ESS® Switch	Network Management Exception page 130 indicates whether an MC1 or MC2 level of congestion has been received.

E. Deactivation

2.11 For all switches, throttling is performed for 4 to 6 seconds unless additional REL messages with the ACCL parameter are received. If this occurs, throttling is performed according to the new ACC level for an additional 4 to 6 seconds. The 4- to 6-second interval cannot be changed by the user. The variation in the interval occurs because of the timing constraints.

NOTE:
If the new ACC level is MC0, the 4ESS switch immediately removes the throttling. The 1A ESS and 5ESS switches will wait for the 4- to 6-second interval to expire before throttling is removed.

Trunk Signaling with Abnormal Network Conditions

2.12 In order to determine the availability of the SS7 trunks, the state of the SS7 signaling network is required. If the far-end switch is unavailable through the SS7 signaling network, all SS7 trunk groups which end at that switch are unavailable for traffic. Each Lucent Technologies switching application dynamically inhibits call originations to a far-end switch that is declared inaccessible. For SS7 signaling, this declaration may take one of the following forms:

(a) A Transfer Prohibited (TFP) message is received from each adjacent STP concerning the far-end node.

(b) The linkset to one of the adjacent STPs is out of service and a TFP message is received from the mate STP concerning the far-end switch.

(c) Both linksets to the adjacent STPs are out of service.

(d) A subsystem prohibited message is received concerning subsystem 3 for the far-end switch. Subsystem 3 is the ISUP subsystem.

(e) Transfer Control (TFC) message is received from an STP indicating Level 2 or 3 congestion for a far-end node.

2.13 When the far-end switch is declared unavailable, one of the following events occurs:

(a) If alternate routing is not defined, the call is given error treatment.

(b) If alternate routing is defined but not selected, the call is given reorder treatment.

(c) If alternate routing is defined and selected, the call is attempted over the alternate route.

The parts that follow describe the mechanism each switching application employs in dealing with far-end office unavailability.

⇒ NOTE:
Alternate Link Set Routing (ALSR) functionality may not follow these comments exactly. See Chapter 3, Part 6 for ALSR.

A. 1A ESS™ Switch—Alternate Routing

2.14 A signaling indicator kept in trunk group translations is dynamically set whenever signaling to the far-end office is prohibited. This indicator, known as the Skip Bit, is reset whenever prohibited signaling destination becomes available again. If the Skip Bit is set, the 1A ESS switch will attempt to use an alternate route.

2.15 In order to determine which trunk groups have dynamically had their Skip Bit set, a request capability is provided to query translations. For more information on this capability, refer to the **VF:RUGRAT** input message (**PC** and **BLOCKED** keywords) in the 1A ESS switch *IM-6A001-01* manual and the **VF24** output message in the *OM-6A001-01* manual.

2.16 Introduced in the 1AE11 generic software release is an option to specify whether to look for alternate routing or to immediately respond with error treatment. This option, implemented in the **RC:TG** recent change message using the **CNTRLT** keyword (the default is "CANCEL_TO"), allows the craft to maintain greater control of the network given a network failure (that is, office isolation) has occurred. The following examples help to show this control.

2.17 In the first example (Figure 2-2), **A** and **B** represent two end offices and **C** represents a local tandem office. Normally, **A** routes traffic to **B** over route **A-B** and overflow traffic is routed through **C** (route **A-C-B**), if necessary.

2.18 For an example, **B** becomes isolated for some reason. **A** detects this (that is, a TFP message is received from both local STPs) and dynamically sets the Skip Bit for each SS7 trunk group routing to **B**. When a call tries to originate from **A** to **B**, call processing detects the Skip Bit being set on the SS7 trunk group and looks at the **CNTRLT** control for the trunk group. If the **CNTRLT** control is set to "cancel to" (that is, 0), the call is routed to route index 180 (No Circuit Announcement). This prevents possible use of resources for calls that would have failed anyway at **C**. Also, **C** does not expend resources attempting to complete a call it cannot complete.

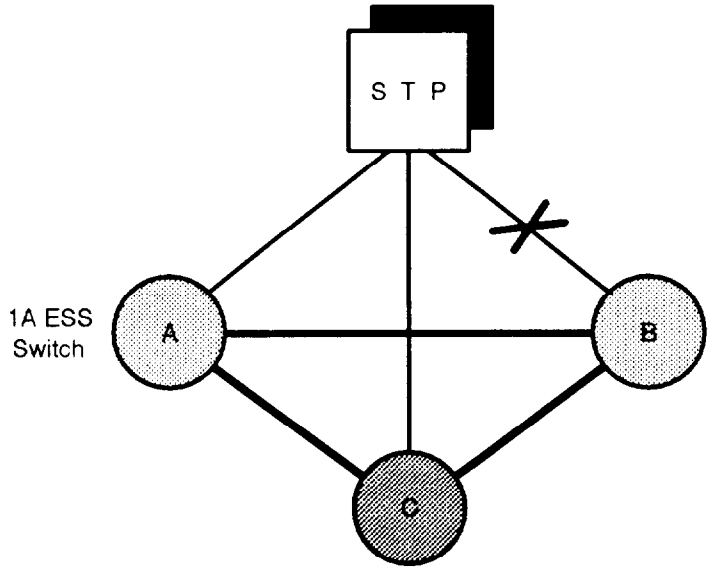


Figure 2-2. Direct Trunks Between End Offices with Overflow to a Local Tandem

2.19 If the **CNTRLT** control is set to "skip routing" (that is, 1), the alternate route (that is, route **A-C-B**) is attempted. Since **B** is isolated, the call fails at **C**. Resources have been utilized to attempt to complete a call that cannot be completed.

2.20 In the second example (Figure 2-3), **A** and **D** represent end offices and **B** and **C** represent local tandem offices. As in the first example, **A** routes traffic to **D** over route **A-B-D** and overflows traffic through **C** (route **A-C-D**), if necessary. Let us say **B** becomes isolated.

2.21 Office **A** detects this and dynamically sets the Skip Bit for each SS7 trunk group routing to **B**. When a call tries to originate from **A** to **B**, call processing detects the Skip Bit being set on the SS7 trunk group and looks at the **CNTRLT** control for the trunk group. If the **CNTRLT** control is set to "cancel to", the call is routed to route index 180 (No Circuit Announcement). In this case, a call is blocked that otherwise would have overflowed to the alternate route (through **C**) and possibly completed.

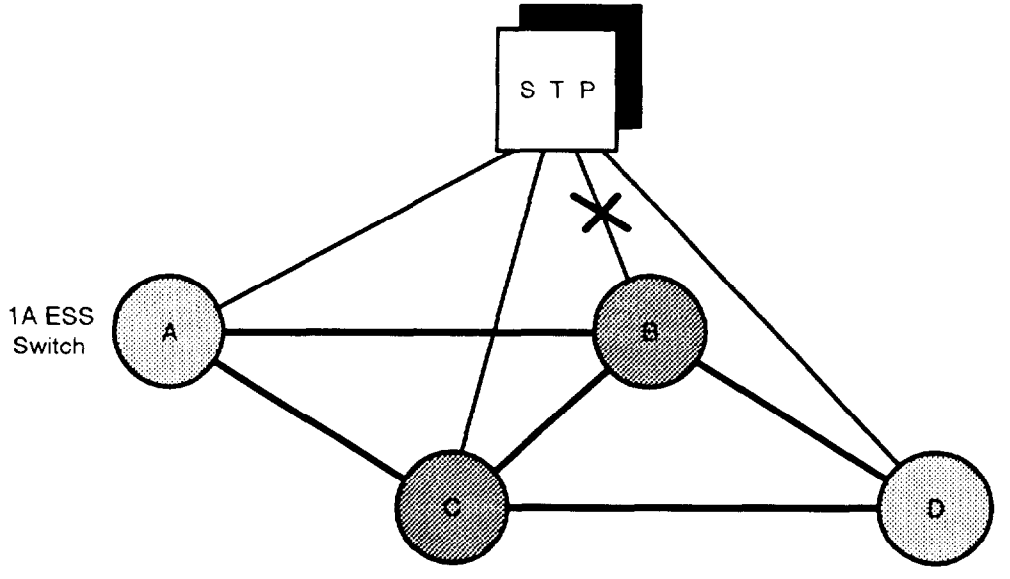


Figure 2-3. Direct Trunks to a Local Tandem with Overflow to Another Local Tandem

2.22 If the **CNTRLT** control is set to "skip routing", alternate route **A-C-D** is attempted. The call then completes normally, oblivious of the fact that **B** is isolated.

2.23 Whether it is preferable to set the **CNTRLT** control to "CANCEL TO" or "SKIP routing" depends on the functionality of the connecting switch. If the connecting switch plays an end office role and no other tandems exist, the **CNTRLT** control should be set to "CANCEL TO." If the connecting switch is a tandem, and other tandems provide an alternate route, the **CNTRLT** control should be set to "SKIP ROUTING". For more information refer to 231-318-375, *Common Channel Signaling System 7 1A ESS Switch*; 231-390-305, *1A ESS Switch Network Management*; and 231-390-502, *Integrated Service User Part, Common Channel Signaling System 7, 1A ESS Switch.*

2.24 In addition to the previously mentioned dynamic controls, the 1A ESS switch allows four manual network management controls:

- **CT-ACT** (cancel to)
- **CF-ACT** (cancel from)
- **RR-ACT** (regular reroute)
- **SK-ACT** (skip).

2.25 Any manual control placed on a trunk group overrides any automatic controls/conditions in place. For more information on these manual controls, please refer to the 1A ESS switch *IM-6A001, Input Message Manual.*

B. 4ESS™ Switch

2.26 When a switch connected to a 4ESS switch (Figure 2-4) is declared SS7 signaling inaccessible, a Machine Congestion Level 3 (MC3) control is applied to all SS7 Trunk Subgroups (TSGs) to the connecting switch. The MC3 control specifies that "no trunk hunt" is to be done on this TSG. Essentially, each SS7 TSG in the routing data block is skipped over in the search for a voice path to the connecting switch. If an available TSG is found, call processing continues. Otherwise, the call is given appropriate final handling treatment.

2.27 When the office is declared SS7 signaling accessible again, the MC3 control is removed and each SS7 TSG to the connecting switch is eligible for trunk hunting again.

NOTE:
Signaling link congestion Levels 2 and 3 do not affect the MC3 control.

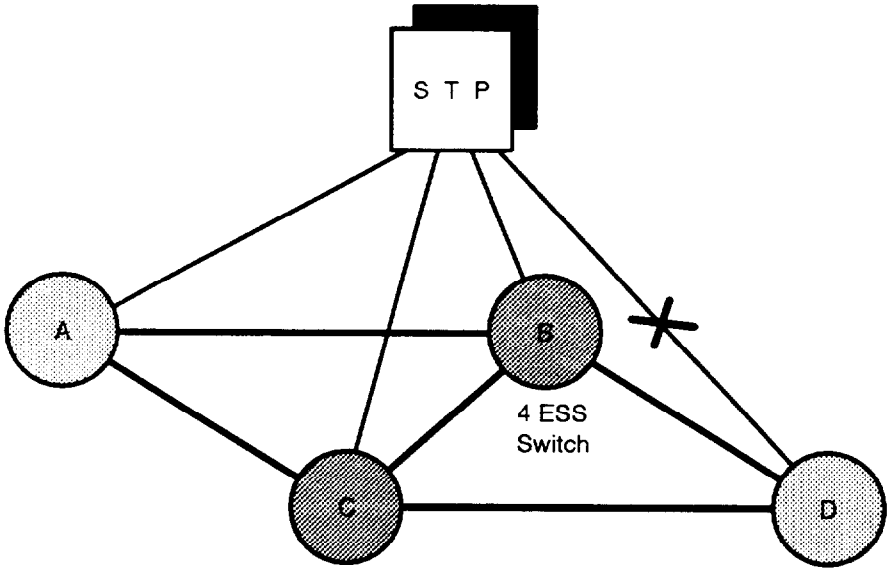


Figure 2-4. Direct Trunks to an End Office With Overflow to Another Local Tandem

C. 5ESS Switch

2.28 For each trunk origination, 5ESS switch call processing checks the status of the far-end switch. If the far-end switch is declared SS7 signaling inaccessible or reaches signaling link Level 2 or 3 congestion, the 5ESS switch inhibits traffic from routing over the trunk group (Figure 2-5). When the switch becomes accessible or the congestion level falls below Level 2, traffic is allowed over the trunk group.

NOTE:
The 5ESS switch does not declare the far-end node inaccessible if a subsystem prohibited message for subsystem 3 (ISUP) is received.

Control Type

2.29 In generic software release 5E8, the field **CONTROL TYPE** was added to RC Views 5.1 (Trunk Group) providing a choice in handling the call when traffic is prohibited over a primary ISUP7 trunk group. The CONTROL TYPE is checked when an outgoing ISUP7 trunk is selected to route out of an office, but the associated SS7 dynamic routing is marked TFP. Before attempting to re-route, the CONTROL TYPE is checked to determine whether to skip the current trunk and attempt alternate routing, and if the call should be canceled without attempting to re-route.

The data administrator is responsible for setting CONTROL TYPE. CONTROL TYPE should be based on the network topology. Guidelines for setting CONTROL TYPE are described in the following scenarios:

(1) CONTROL TYPE should be set to **"CANCEL"** if the far-end office **only uses** ISUP7 trunks, but the ISUP7 trunks are not accessible due to a failure. Under these conditions calls should not be re-routed because the far-end switch cannot accept incoming calls, and re-routing calls could possibly cause congestion on the indirect routes.

(2) CONTROL TYPE should be set to **"SKIP"** if the available alternate routes do not use ISUP7 signaling. Although the far-end switch is not accessible using ISUP7 trunks, non-ISUP7 trunks may be able to reach the far-end switch and complete the call.

(3) CONTROL TYPE should be set to **"SKIP"** if dual tandems are connected to a far-end office. Although the first tandem may not be able to reach the far-end office, via ISUP7, the second tandem may have non-ISUP7 signaling that is capable of routing the traffic.

2.30 In addition to the dynamic control already mentioned, the 5ESS switch allows five manual network management controls to be set on a trunk group level, via two input messages:

- **SET:TGC** (skip, cancel to, cancel from, cancel reroute overflow)
- **SET:RR** (manual reroute).

2.31 Any manual control placed on a trunk group overrides any automatic controls/conditions in place. For more information on these manual controls, please refer to 235-600-700, *5ESS Switch Input Message Manual.*

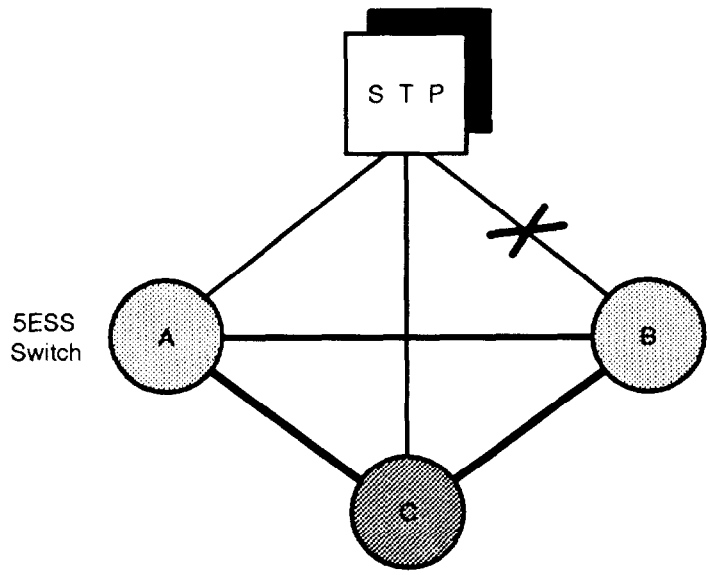


Figure 2-5. Direct Trunks to an End Office with Overflow to Another Tandem

3. Link and Facility Activation Procedures

3.01 Linking up to the network is the process of successfully establishing a Signaling Link (SLK) between a signaling point (for example, switch or Service Control Point) and an STP. When the link connection is successfully established, both ends of the SLK show it as available and in service. The signaling link is capable of transporting Level 2 of the SS7 protocol and has passed a signaling Level 3 transport test. The Level 3 transport test is called the Signaling Link Test (SLT). This does not necessarily mean that all level 3 messages are properly routed, but indicates the ability is present to successfully transport them if the routing data is set up properly.

3.02 The process of activating a signaling link is a series of steps that must be completed before the link is established.

(1) Installation personnel must successfully complete the installation of the Common Network Interface (CNI) and Digital Facility Access (DFA) frames/cabinets.

(2) The Local Exchange Carrier (LEC) may perform preactivation testing that involves establishing Level 2 of the SS7 protocol.

(3) At the time of link activation, both ends of the SLK must coordinate their activities to establish an active signaling link.

3.03 The CNI subsystem provides a major and minor state for each signaling link. As a signaling link progresses through each of the activation steps, it may change one or both of these states. Table 2-D lists the valid combinations of the SLK major and minor states.

Table 2-D. CNI Valid Combinations for SLK Major and Minor States

Major State	Minor State	Description
AVL	IS	Available—Link is available for service. In Service—Link is operating normally and passing data.
AVL	MOOS	Available—Link is available for service. Manually Out-Of-Service—Link is manually removed from service with a **CHG:SLK** input message.
AVL	OOS	Available—Link is available for service. Out-Of-Service—Link is removed from service by a CNI process.
UNAV	GROW	Unavailable—Link is not available for service. Growth—Link is being added to the system and is available for diagnostics.
UNAV	TEST	Unavailable—Link is not available for service. Test—Link is unavailable for normal use. This state is used during testing for sending test messages only. It is the same as UNAV GROW except that link ACTIVE/OOS timers are administered.
UNEQ	none	Unequipped—No signaling link exists.

3.04 Each switch or *A-I-Net* advanced intelligent network products STP provides a status page that can be used to determine the current CNI major and minor states of its signaling links. Table 2-E provides a cross-reference.

Table 2-E. Signaling Link Status Pages/Views

1A ESS™ Switch	4ESS™ Switch	5ESS® Switch	*A-I-Net*® STP	*A-I-Net* SCP
Page 1108	Page 1108	Page 1521	Page 1141, Page 1142	Page 116 Page 1160

3.05 Failure to successfully establish the signaling link can be the result of no connectivity, signaling link errors, or a failure of the Level 3 test (SLT). To isolate the source of the failure, please refer to "Signaling Link Trouble" in Chapter 4.

Installation

3.06 Prior to any actions by the operating company to do preactivation testing or actual activation, the installation of the CNI and DFA equipment in the switch must be successfully completed.

3.07 Successful installation of the CNI and DFA hardware and software accomplishes several things necessary to the activation process. First, the link nodes are fully diagnosed and pass all diagnostics. As a result, the signaling link is tested from the switch out to the Digital Service Unit (DSU) in the DFA frame/cabinet.

3.08 Second, the DSU options in each DSU should be properly set. Table 2-F should be used to set the 12-position option dip switch on the Lucent Technologies 2556 DSU. On earlier 2556 DSU boards, the dip switch is enabled when in the OFF position and disabled when in the ON position. Newer DSU boards are marked OPTION ENABLE. When the dip switch is set toward the OPTION ENABLE label, it is enabled. If set away from the OPTION ENABLE label, the dip switch is disabled.

Table 2-F. Lucent Technologies 2556 Digital Service Unit Option Settings

Position	Setting	Description
1	Enable	Remote Digital Loopback
2	Disable	Elastic Store
3	Enable	Data Mode
4	Disable	Circuit Assurance
5	Disable	System Status
6	*	Timing Options
7	*	Timing Options
8	Disable	Streaming Terminal
9	Enable	Continuous Request-To-Send
10	Enable	56 kbps Speed Option
11	Enable	56 kbps Speed Option
12	Enable	56 kbps Speed Option

* If the 2556 DSU is connected to a D4 channel bank, positions 6 and 7 should be disabled. For applications where internal timing is necessary, position 6 should be enabled and position 7 should be disabled. For applications where external timing is necessary, positions 6 and 7 should be enabled.

3.09 In addition to the option dip switch, the Local Loopback (LL) controlled through Data Terminal Equipment (DTE) Connector strap plug should be in the enable position. This allows an **LL** test to be controlled from DTE attached to the DSU DTE connector.

3.10 For more information concerning the Lucent Technologies 2556 DSU and its option/plug settings, refer to the 999-100-188, ***Dataphone**** *II 2500-Series Data Service Units User's Manual.*

3.11 Finally, the SLK should be in the Unavailable Growth (UNAV GROW) state.

Preactivation Procedures

3.12 After installation personnel has completed work on the CNI and DFA hardware and software, the operating company must complete certain functions prior to the actual link activation. These functions include:

(a) Ensuring proper CNI data (Table 2-G) is inserted for the following views/functions:

Table 2-G. CNI Data for Switch Views/Functions

1A ESS™ Switch Page 1105	**4ESS™ Switch DMS* Function**	**5ESS® Switch RC/V View**	***A-I-Net®* STP DMS Function**
OFDATA	OFDATA	View 15.1	SELFID LNKSET
LKDATA	LKDATA	View 15.2	LNKDAT
* DMS means Data Management System.			

NOTE:
Refer to Chapter 3, "Elements of an SS7 Network" for details on populating the above views/functions.

(b) Verifying that the proper DSU options are set in the DFA frame/cabinet. Refer to Chapter 4, "Digital Service Unit End-to-End Testing," for further details.

(c) Verifying that the DSUs are not looped locally or remotely.

(d) Properly connecting the DFA to the carrier facility and verifying the carrier end-to-end.

(e) The office can set up monitoring of the SLK for preservice testing using the Unavailable Test (UNAV TEST) state of the SLK. This state provides link data to the user without generating alarms or allowing the SLK to interact with the network. Level 2 of the SS7 protocol is brought up but no CNI timers are administered.

3.13 The link nodes should be in the Active (ACT) state with the SLKs in the UNAV GROW state prior to the preactivation procedures. This monitoring is accomplished by the following steps:

(1) Turn on the SLK monitor with the **MON:SLK** input message.

(2) Put the SLK in the UNAV TEST state with the **CHG:SLK** input message. The following message should appear on the Receive-Only Printer (ROP):

CHG SLK a b COMPL
SLK a b CHANGE ACCEPTED, NEW MINOR STATE = TEST.

⇒ NOTE:
The far-end office SLK must also be in the UNAV TEST state.

(3) The SLK is synchronized and prove-in executed when the following output message is received:

REPT MON SLK
SLK a b c UNA TEST d

where: **a b** = group and member numbers
c = far-end *Common Language** CLLI code
d = value of real-time clock

(4) On satisfaction of operating company personnel that link prove-in is successful, the SLK monitor can be turned off with the **MON:SLK** input message.

(5) End-to-end error rate testing should be completed either at the digital test center or through DSU end-to-end testing.

---

* *Common Language* is a registered trademark and CLEI, CLLI, CLCI, and CLFI are trademarks of Bell Communications Research, Inc. (See Chapter 3, Part 4 for CLLI code treatment).

Activating the Signaling Link

3.14 When a signaling link is to be activated, the switch should coordinate with the STP to put the signaling link in the AVAILABLE-IS state with the following steps:

(1) DSU end-to-end tests should be completed from both ends of the SLK.

(2) Both ends of the SLK must have their link nodes ACT and the SLK major state should be changed from the unavailable (UNAV) to available (AVL) state. The SLK major state is changed via the RC view/functions listed in the following table.

Table 2-H. Signaling Link Recent Change View/Functions

1A ESS™ Switch Page 1105	4ESS™ Switch DMS Function	5ESS® Switch RC/V View	*A-I-Net*® STP DMS Function
LKDATA	LKDATA	15.2	LNKDAT

⇒ NOTE:
Refer to Chapter 3, "Elements of an SS7 Network" for details on populating the above views/functions.

(3) On successful SLK prove-in and SLT exchange as shown in Figure 2-6, the SLK automatically changes state to Available In Service (AVL IS). The signaling link is now active.

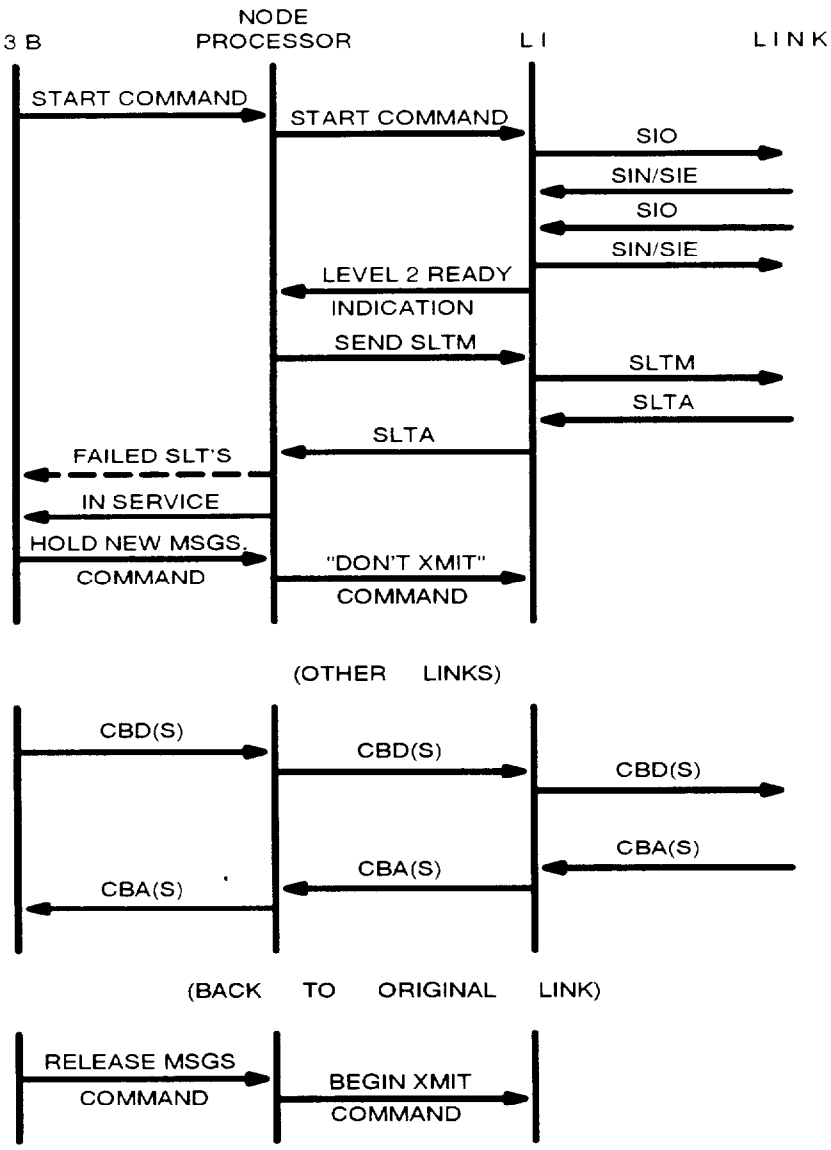


Figure 2-6. Signaling Link Activation

4. Trunk Conversion

Manual Conversion

4.01 The PTS trunk conversion process involves deleting each trunk from the switch PTS trunk group and reinserting it in a new SS7 trunk group. The following guidelines should be followed before commencing with the actual trunk conversion process:

(a) The CNI ring and signaling links to the STPs are operational and all tests have passed.

(b) The CNI office, link, and routing data views or functions are appropriately populated.

(c) The STPs are updated with the point codes and other data relating to the offices between which the trunks are connected.

(d) The office is properly engineered for Voice Path Assurance (VPA), or Continuity Check, circuits and these circuits are installed.

(e) Since the conversion is being done to trunks that are already in use, the trunk hardware must pass all tests and currently be operational.

(f) The conversion of trunks or trunk groups requires coordination in both offices connected by the trunks so that both ends of the trunks are converted to SS7 at about the same time. If only one end of the trunk is converted, calls cannot complete and diagnostics fail.

(g) To avoid loss of traffic, the conversion should be made during a low traffic period.

(h) SS7 trunk data needs to be properly provisioned (for example, Glare, Trunk Hunting, and so forth).

4.02 Before placing the new SS7 trunk(s) into service, it is recommended that the following tests be performed:

(a) A trunk translations test should be run for each trunk member. This test ensures that the far-end switch knows about the Trunk Circuit Identification Code (TCIC) value assigned to each trunk. Refer to Chapter 3, "Trunk Translation Test," and Chapter 6, "Circuit Validation Test," for additional information concerning this test.

(b) An SS7 trunk query should be run for each trunk member. This essentially marks each trunk state blocked at both ends. Refer to Chapter 6, "Circuit Query," for additional information about query.

(c) A VPA (or Continuity Check) test should be run for each trunk member. This tests the voice path for quality transmission. Refer to Chapter 3, "VPA/Continuity Check Circuits," for additional information about this test.

(d) An operational test call should be placed over each trunk. If the trunk fails the test call, the problem is likely to be in the data of either the near-end or far-end office.

The section that follows includes application specific information about the manual trunk conversion process.

A. 1A ESS Switch

4.03 The 1A ESS switch provides a recent change message, **RC:TKCNV7**, that moves trunks with PTS signaling (TYPE 1, 2, 10, or 15 trunk group) to one with SS7 signaling, or vice versa. The message allows trunks to be moved directly from one working Trunk Group (TG) to another TG without going through trunk group zero.

4.04 For the specific 1A ESS switch procedure regarding manual trunk conversion, refer to 231-318-375, *Common Channel Signaling System 7 1A ESS Switch.*

4.05 In addition, a request capability is provided to verify that the TG has been moved. Refer to the **VF:TAG** input message (**CCS7TG** keyword) and the **VF04** output message in the IM-6A001 and IM-6A002, *1A ESS Switch Input Message Manual,* and OM-6A001, *1A ESS Switch Output Message Manual.*

B. 4ESS™ Switch

4.06 The 4ESS switch has two procedures for converting a TSG from MF to SS7 signaling. The procedures differ in whether the TSG remains in service or is removed from service during the conversion process. The following describes each procedure.

⇒ NOTE:
For additional explanation of input/output and recent change messages referenced in these procedures, refer to the 4ESS switch *IM-4A000-01* and *OM-4A000-01* manuals and the TG-4, *Translation Guide.*

Trunk Subgroup Remains in Service

4.07 The following procedure applies when the TSG being manually converted from MF signaling to SS7 signaling remains in service during the conversion process.

(1) Verify the TSG characteristics using the **VER:TSG** input message. This message provides the information for populating RC Form 100 in Step 4.

(2) Verify the TSG member (trunk) assignments using the **VER:TRK** input message (**TAN** keyword). This message provides the detailed office assignments of each TSG member. The Traffic Number (TFN) and Trunk Appearance Number (TAN) are required when populating RC Form 203.

(3) Verify the SS7 dynamic routing status in the 3B/CNI processor using **OP:C7NET** input message (**ROUTING** keyword) to ensure that the cluster being converted has CNI routing before proceeding any further. Refer to Chapter 6, "Displaying Routing Data (OP:C7NET)," for additional information on this input message.

(4) Create a new TSG with ISUP signaling. Use of the appropriate RC form (Table 2-I) depends on the directionality of the TSG as follows:

Table 2-I. Recent Change Form

RC Form	Trunk Direction
100	2-way
101	1-way incoming
102	1-way outgoing

The name of the new TSG should be the same as the old TSG except for the Near Building Subdivision. The Trunk Circuit Identification Code should equal the TFN of the TSG member. Other TSG characteristics deserving special attention include: PCF, DPC, TOT, ISC, OSC, CCIS2WIRE, XCPA, REV, GLARE, and EAS.

(5) Verify the TSG characteristics using the **VER:TSG** input message.

(6) Identify all of the Routing Data Blocks (RDBs) that contain the old TSG using the **VER:RDBLIST;ALL** input message (**CIN** keyword).

(7) Add the new TSG to all the RDBs that contain the old TSG using RC Form 513. The new TSG should be installed above the old TSG in all the RDBs.

(8) Verify all of the RDBs to ensure that the new TSG is added above the old TSG and that both TSGs have the same characteristics. The **VER:RDB** input message (**RDBI** keyword) should be used to accomplish this.

(9) Coordinate the conversion with the far-end switch to ensure that they are ready to turn down the TSG members and proceed with the conversion.

(10) Remove as many TSG members from service as allowed using the **SET:TRKSTAT** input message (**CAD.DSA** and **CIN** keywords).

(11) Remove the TSG members identified in Step 10 from the old TSG using RC Form 202.

(12) Add the TSG members removed in Step 11 to the new TSG using RC Form 203.

(13) Verify the TSG member assignments using the **VER:TRK** input message (**TAN** keyword).

(14) Coordinate with the far-end switch before proceeding past this point. The far-end switch must be ready to test the members before you proceed.

(15) Test the TSG members for correctness and workability for the following areas using the **TEST:TRK** input message:

— Call Processing and Maintenance states: **CIN** and **TQU** keywords

— Traffic Number, Office Name, and Trunk Glare: **CIN** and **TIC** keywords

— Voice Path Assurance: **CIN** and **CCK** keywords.

(16) Coordinate with the far-end switch and activate the members just added to the new TSG using the **SET:TRKSTAT** input message (**ACT** and **CIN** keywords).

(17) Repeat Steps 9 through 16 for each group of TSG members to be converted. When all the members are activated in the new TSG you can proceed with the next steps.

(18) Remove the old MF TSG from all of the RDBs using RC Form 514.

(19) Delete the old MF TSG using RC Form 107.

(20) If the ISUP TSG requires the name of the old TSG, change the new TSG name to the old TSG name using RC Form 802. This RC Form changes the TG name so the TSG must equal the TG. If the TSG is only part of the TG, you must create a second new ISUP TSG with the correct name and move all the members to it.

(21) At this point, the TSG is converted from MF signaling to ISUP (that is, SS7) signaling. You are ready to proceed with the next TSG to be converted.

End of Procedure.

Trunk Subgroup Removed From Service

4.08 The following procedure applies when the TSG being manually converted from MF signaling to SS7 signaling is removed from service during the conversion process.

(1) Verify the TSG characteristics using the **VER:TSG** input message. This message provides the information for populating RC Form 107 in Step 7.

(2) Verify the TSG member assignments using the **VER:TRK** input message (**TAN** keyword). This message provides the detailed office assignments of each TSG member. The TFN and TAN are required when populating RC Form 203.

(3) Verify the SS7 dynamic routing status in the 3B/CNI processor using the **OP:C7NET** input message (**ROUTING** keyword). We want to ensure that the cluster being converted has CNI routing before proceeding any further. Refer to Chapter 6, "Displaying Routing Data (OP:C7NET)," for additional information on this input message.

(4) Coordinate the conversion with the far-end office whose trunks are being converted before proceeding any further.

(5) Remove the TSG members from service (CAD.DSA State) using the **SET:TRKSTAT** input message (**CAD.DSA** keyword).

(6) The TSG members must be removed from the TSG in order to change the signaling characteristics. The removal is accomplished with RC Form 202.

(7) Change the TSG characteristics to indicate ISUP signaling. The TSG characteristics noting attention include: PCF, DPC, CIN, TOT, ISC, OSC, CCIS2WIRE, XCPA, REV, GLARE, and EAS. Use of the appropriate RC Form depends on the directionality of the TSG as shown in Table 2-I.

(8) Verify the TSG characteristics using input message **VER:TSG**.

(9) Add the members back to the TSG using RC Form 203.

(10) Verify the TSG member assignments using the **VER:TRK** input message (**TAN** keyword).

(11) Coordinate with the far-end switch before proceeding past this point. The far-end switch must be ready to test and activate the members before you proceed.

(12) Test the TSG members for correctness and workability for the following areas using the **TEST:TRK** input message:

- — Call Processing and Maintenance states: **CIN** and **TQU** keywords
- — Traffic Number, Office Name, and Trunk Glare: **CIN** and **TIC** keywords
- — Voice Path Assurance: **CIN** and **CCK** keywords

(13) Coordinate with the far-end switch and activate the TSG members using the **SET:TRKSTAT** input message (**ACT**, **CIN**, and **TSG** keywords).

(14) At this point, the TSG is converted from MF signaling to ISUP (that is, SS7) signaling. You are ready to proceed with the next TSG to be converted.

End of Procedure.

C. 5ESS Switch

4.09 In the 5ESS switch, the following is a guide for performing the necessary Recent Changes for manual trunk conversion:

(a) Review the trunk member data and hold values in memory for an automatic operations support system. The quantity field in RC view 5.5 may be used.

(b) Delete the designated PTS trunks that are already out-of-service using recent change view 5.5.

(c) Create the new SS7 group, or update the PTS group with SS7 data using recent change view 5.1. The PTS trunk group to be updated would be a TG with all members deleted.

(d) Insert the new SS7 members using data from review of old member after the update of the proper value pairs. RC view 5.10 (trunk copy) may be used for this action.

The above steps should be repeated for each trunk in the trunk conversion block.

4.10 For the specific 5ESS switch procedure regarding manual trunk conversion, please refer to 235-190-120, *5ESS Switch Common Channel Signaling Features.* For specific trunk test procedures using Circuit Maintenance System (CMS), refer to the *234-103-series* of Lucent Technologies practices.

Automated Conversion

4.11 Simultaneous Trunk Conversion via Automatic Recent Change (STAR) provides for the automated conversion of trunks from PTS protocol to SS7 protocol. It also provides a method of verifying the trunk network number and/or trunk equipment number connectivity between two switching offices.

4.12 One of two switching offices is designated to control the STAR process. This office is called the HOST office. The connecting office is designated as the REMOTE office.

4.13 STAR services can be executed between any of the following switch combinations:

- Two 1A ESS switches
- A 1A ESS switch and a 5ESS switch
- Two 5ESS switches.

4.14 If the conversion is to be performed between a 1A ESS switch and a 5ESS switch, either switch type may be designated as the HOST office.

4.15 Supported generic software releases for STAR services include 1AE10 or later for 1A ESS switches and 5E4.2 or later for 5ESS switches.

A. Prerequisites

4.16 To operate the STAR program the following prerequisites must be met:

(a) Since the HOST office controls the conversion process, only 2-way PTS trunks and 1-way outgoing (from the HOST office) PTS trunks may be selected for the STAR process. One-way incoming PTS trunks can be converted to SS7 trunks by reversing the roles of the HOST and REMOTE offices and running STAR on those trunks.

(b) Before the STAR process can be initiated, both the HOST and the REMOTE switches must be preconditioned. Refer to 256-015-310, *Simultaneous Trunk Conversion*, changes for 1A ESS or 5ESS switches for this information.

B. Operation

4.17 The craft is allowed four STAR options:

(a) One trunk per STAR request can be converted.

(b) One trunk group per STAR request can be converted.

(c) A trunk group conversion attempt can be stopped.

(d) A trunk group conversion attempt that is stopped can be restarted.

4.18 During a STAR session the HOST office automatically places test calls to the REMOTE office to determine connectivity between offices. The REMOTE office detects the test call and responds with connectivity data back to the HOST office. From the response the HOST office assembles appropriate RC input messages for itself and the REMOTE office in order to convert the trunk from PTS protocol to SS7 protocol. The HOST RC request is processed internally while the REMOTE RC request is sent over a dedicated data link to the REMOTE office for processing. This cycle is repeated for each designated trunk or trunk group to be converted.

C. Limitations and Restrictions

4.19 The following list addresses the limitations and restrictions of STAR.

(a) Only one trunk is converted at a time.

(b) Only PTS trunks are supported for conversion.

(c) STAR does not support changes to the trunk direction during conversion.

(d) STAR does not support the combination of multiple trunk groups into a single trunk group during conversion.

(e) STAR does not support the conversion of trunk groups with Software Carrier Group Alarms assigned.

NOTE:
Service Order and other Recent Changes need not be inhibited by STAR operation.

D. Benefits

4.20 The STAR service provides the following benefits:

(a) It automatically converts trunks between any combination of 1A ESS and 5ESS switches.

(b) Once completed, nothing else needs to be done. Each trunk will continue to carry the full array of normal and custom services originally associated with it along with its new SS7 capabilities.

(c) It is a switch resident operation. Once loaded via library tape into switch memory, the program runs at machine speed. There is Input/Output (I/O) channel contention.

(d) The process uses resident switch data. It requires no data conversion or record scrubbing. Not only does this save time and effort, it ensures greater accuracy by eliminating a primary cause of error introduction.

(e) It allows normal RC activity to continue without interruption.

(f) It automatically produces an output file that contains a complete record of all trunk conversion activity. This file can become the new office record update.

(g) A single trunk conversion can be performed faster compared to manual conversion.

(h) It can initiate additional conversion activity once the process has begun, generating an effective rate of approximately four trunks complete per minute.

Data Administration Guidelines

3

Contents Page

Contents Page

Contents Page

Contents Page

Contents Page

Contents Page

Data Administration Guidelines

3

1. Introduction

1.01 Integrated Services Digital Network—User Part (ISUP) signaling can initiate, set up, supervise, and disconnect basic interoffice Signaling System 7 (SS7) calls. This is accomplished by sending and receiving signaling messages through the SS7 network (Figure 3-1).

1.02 The ISUP signaling messages are circuit related and provide information that puts SS7 trunks into valid states for call processing and trunk maintenance. Successful execution of call processing and trunk maintenance functions requires that certain elements of the SS7 trunk-related data be consistent among connecting switches in the Local Exchange Carrier (LEC) network.

1.03 In addition, routing of circuit-related signaling messages requires consistency throughout the network for some key switches and Common Network Interface (CNI) data values. This includes point Code (PC), Trunk Circuit Identification Code (TCIC), *Common Language** CLLI code, Voice Path Assurance (VPA) Type and Rate, Frequency of Testing, Glare Control, Hunt Direction, Link Data, Cluster Data, and Selected Timers.

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

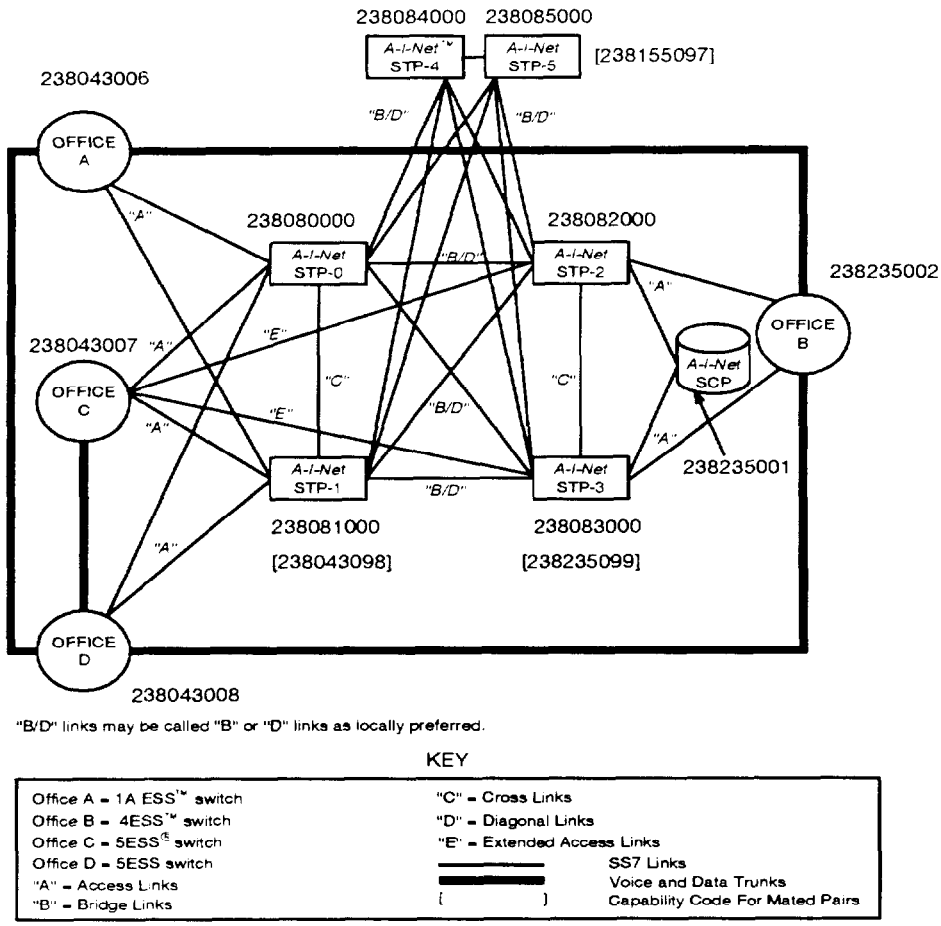


Figure 3-1. Sample LEC Network Configuration

Network Impact on CNI Lucent Technologies Switch Products and *A-I-Net*® Advanced Intelligent Network Products STP Data

1.04 Much of the data applicable to Per-Trunk Signaling (PTS) is still valid for ISUP. However, the introduction of the SS7 has resulted in the development of some new translation structures and requires population of these translation structures with information that affects network functionality.

1.05 For clarification, translation data is office data residing in a particular switch. For the 1A ESS™ switch, translations data includes the Translations Data Assembly (TDA) and Parameters information that resides in the 1A Processor. For the 5ESS® switch, translations data includes the Office Dependent Data (ODD) which resides in the Switching Modules (SMs) and/or the Administrative Module (AM).

1.06 In contrast, CNI data relates to functions provided by the CNI ring. It is separate from office specific data stored in the switch. In the 1A ESS and 4ESS™ switches, CNI data resides in an Attached Processor System (APS). In the 5ESS switch, CNI data resides in the AM. In the *A-I-Net* products Signaling Transfer Point (STP), the CNI data resides in the Lucent Technologies 3B20D computer.

1.07 The functionality of the SS7 network based features depends on both the existence and consistency of key office and CNI data, as well as STP data values. The following sections identify these data elements and explain from the network perspective the usage of the data and how the items should be populated.

1.08 A summary of the required Recent Change (RC) views/functions is shown in Table 3-A and Table 3-B.

⇒ NOTE:
The "Office" data type relates to the trunks and the "CNI" data type relates to the signaling links.

Table 3-A. Recent Change Views/Functions for Consistent ISUP Data

Consistency Item	Data Type	1A ESS™ Switch	4ESS™ Switch	5ESS® Switch	*A-I-Net*® STP
Point Codes	Office	RC:POINTC RC:TG RC:TKCNV7 RC:TGMEM	RC:TSG	View 5.1	N/A*
Trunk Circuit Ident. Code (TCIC)	Office	RC:TKCNV7 RC:TGMEM RC:TMBCGA	RC:TRK	View 5.5	N/A
CLLI† Code	Office	See ‡	RC:TSG RC:TRK	View 5.1	N/A
VPA	Office	RC:PSWD	RC:TRK RC:TSG	View 5.1 View 14.1	N/A
Glare	Office	RC:TG	RC:TSG	View 5.1	N/A
Hunt Direction	Office	RC:TG	RC:TSG:	View 5.1	N/A

* N/A means not applicable.

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

‡ In the 1A ESS switch, the point pode and the CLLI code of the local office are stored in Parameters, not Translations.

Table 3-B. Recent Change Views/Functions for Signaling Data

Consistency Item	Data Type	1A ESS™ Switch	4ESS™ Switch	5ESS® Switch	*A-I-Net*® STP
Point Codes	CNI	OFDATA LKDATA	OFDATA LKDATA	View 15.1 View 15.2	SELFID LNKSET
CLLI Code	CNI	OFDATA LKDATA	OFDATA LKDATA	View 15.1 View 15.2	SELFID LNKSET
Cluster Data	CNI	RC:CNI;xxx ROUTE	CLSROUT* ROUTE†	View 15.9	ORDRTE
Link Data	CNI	LKDATA	LKDATA	View 15.2	LNKSET LNKDAT

* Only for cluster routing

† For Alternate e-links.

2. Elements of an SS7 Network

NOTE:
This section is only an introduction to SS7 and does not include all possible options for using SS7 signaling. For a detailed specification of SS7, refer to TR-NWT-000246, *Bell Communications Research Specifications of Signaling System Number 7.*

2.01 An SS7 network allows signaling information to be transmitted between Signaling Points (SP) [for example, 1A ESS switch, 4ESS switch, 5ESS switch, and *A-I-Net* products Signaling Transfer Point (STP)]. This signaling information controls basic interswitch calls and handles such calling features as Local Area Signaling Services (LASS) and Service Switching Point (SSP) 800 Service.

2.02 The transmission of signaling messages is accomplished via digital Signaling Links (SLKs) which are separate from the channels over which voice and data communications are transmitted. These signaling messages can originate from a Lucent Technologies switch using a CNI to provide access to the SS7 signaling network.

NOTE:
For the purposes of this document, the terms "switch" and "switching system" include the SS7-related functions provided by the CNI.

The messages are routed over SLKs to an STP. The STP, acting as a specialized packet switch, routes signaling messages to outgoing SLKs based on DPC, and from there, they are routed to an SP [another switch, another STP, or a Service Control Point (SCP)].

2.03 The SCP is a centralized data base that provides special call routing instructions needed for some SS7-based features.

2.04 The STPs are engineered in mated pairs. "**A**" (Access) links connect switches to each of a local (home) STP pair. Communication and routing between a mated pair occur via "**C**" (Cross) links. The mated pair concept provides reliability in the network; if one STP fails, the other is capable of handling all the traffic routed to the pair. Engineering of links from the switches to each of the STPs also allows a switch to continue signaling should an STP become inaccessible. The STPs also can process Global Title Translation (GTT) requests and handle low level link and link-routing SS7 messages.

2.05 Frequently, an LEC network is configured using a multiple pair arrangement of STPs. Here, local and remote mated pairs perform routing functions. "**B**" (Bridge) or "**D**" (Diagonal) links connect the mated pairs (see Note).

⇒ NOTE:
LECs with hierarchal networks interconnect local STPs to regional STPs with "**D**" links. Pairs of STPs of the same level are interconnected with "**B**" links.

2.06 The LECs with hierarchical networks interconnect local STPs to regional STPs with "**D**" links. "**E**" (Extended Access) links connect a Lucent Technologies switch to each of a pair of Remote STPs, to provide additional network reliability. Pairs of STPs of the same level are interconnected with "**B**" links. The "**A**", "**B**", "**C**", "**D**", "**E**" links transfer data at a rate of 56 kbps.

2.07 An example of a LEC network configuration using Lucent Technologies products is shown in Figure 3-1. This example and associated data are used throughout this chapter. The network data is shown in the example **OP:C7NET** output in Chapter 6, "Displaying Routing Data (**OP:C7NET**)." For a further description of SS7 network elements, refer to 256-002-100, *Switching Products, Common Channel Signaling 7, Information Guide.*

3. Point Code Assignments

Definition and Use in the SS7 Network

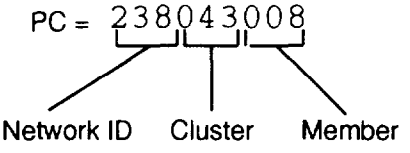
3.01 Point Codes (PCs) are the means by which signaling points in the SS7 network are uniquely identified. These signaling points could be switches, Signaling Transfer Points (STPs), Service Control Points (SCPs), and so forth. The PCs provide the address information (for example, identification of originating and terminating point) that is used to route signaling messages throughout the network. Each switch stores Point Code data in its respective translation structures to identify the far-end offices to which its SS7 trunk facilities are connected. (All SS7 network nodes require Point Code data for signaling routing.) Because of these critical roles, Local Exchange Carriers (LECs) must ensure that Point Code assignments are both correct and unique within their network.

3.02 While there are several standards for Point Code format, LECs should use the American National Standards Institute (ANSI) Bellcore convention. For further information on this requirement, refer to TR-NWT-000246, *Bell Communications Research Specifications of Signaling System Number 7.* Each Point Code is a 9-digit representation having three subfields:

- A 3-digit network identifier
- A 3-digit cluster number
- A 3-digit cluster member number.

3.03 In a 4ESS switch, ANSI should be indicated as the PC format when entering the PC on **RC-TSG** Forms.

3.04 The Network Identifier (NID) is assigned by the network administrator (Bellcore). In large networks, both the Cluster and Cluster Member numbers are assigned by the LEC network signaling administrator. In small networks, the Cluster number is assigned by Bellcore. An example of a 9-digit Point Code is shown below:



3.05 In addition to NID, Cluster, and Cluster Member, several other terms are used when populating Point Code data. Near-end, local, and originating are terms often used synonymously when referencing the "Home" switch or local signaling point. Similarly, far-end, destination, and terminating are three terms used when referencing a connecting switch or signaling point.

Sources of Point Code Information

3.06 Point Code information is stored in SS7 translation data structures. For the 1A ESS and 5ESS switches, the PCs are assigned on a trunk group basis. For the 4ESS switch, the far-end PCs are assigned on a trunk subgroup basis (see Note). However, all trunk subgroups to the same switch must have the same PC.

NOTE:
A trunk subgroup in the 4ESS switch equates to a trunk group in the 1A ESS and 5ESS switches.

3.07 Point Code information is also stored in the CNI data bases, as well as in data bases of other Network Elements (for example, *A-I-Net* products STPs and SCPs). To provide signaling message routing, CNI Point Code data identifies:

- The specific LEC network involved
- The local signaling point (switch or *A-I-Net* products STP)
- The signaling point at the far-end of the SLKs (that is, for a switch or SCP, these are the PCs of the local STPs; for an STP, these are PCs of the connecting STPs, switches, or SCPs).

When populating PC data, refer to Table 3-A for a summary of the recent changes.

Requirements for Populating Point Code Data

3.08 Besides adhering to the ANSI format convention, LECs need to adhere to the following requirements when populating Point Code information:

(1) The Point Code that other network signaling points use to reference a given switch, STP, or SCP must agree with the Point Code that the given switch, STP, or SCP uses to identify itself. Capability codes for STPs are an exception to this rule.

(2) The value of the NID, as assigned by Bellcore, must fall within the range of **001** to **254** to be valid. However, the assigned value is indicative of the network type. Small networks use NID **001** through **004**; large networks use the range **006** through **254**. NID **005** is reserved for Point Code blocks.

(3) For large networks, the value of the Cluster number must fall within the range of **000** to **255**. For small networks, the valid range is **001** to **255** as assigned by Bellcore.

(4) The value of the Cluster Member number must fall within the range **000** to **255**. In large networks, *A-I-Net* products STPs are assigned "**000**" as the value for the Cluster Member. Other network elements must be assigned a nonzero value for Cluster Members.

3.09 Table 3-C shows an example of populating Point Code values for ISUP routing in the sample LEC network configuration shown in Figure 3-1.

Table 3-C. Example Point Code Information for ISUP Signaling

Signaling Point	Local PC	PCs in SS7 Trunk Translations	PCs in CNI Data Base
Office A 1A ESS™ Switch	238043006	Office D = 238043008 Office B = 238235002	NID = 238 Far End PCs: 238080000
Office C 5ESS® Switch	238043007	Office D = 238043008	NID = 238 Far End PCs: 238080000 238082000 238083000
Office D 5ESS Switch	238043008	Office C = 238043007 Office B = 238235002 Office A = 238043006	NID = 238 Far End PCs: 238080000
Office B 4ESS™ Switch	238235002	Office D = 238043008 Office A = 238043006	NID = 238 Far End PCs: 238082000
A-I-Net® STP-0	238080000 Capability Code 238043098	Not Applicable	NID = 238 Far End PCs: 238043006 238043007 238043008 238081000
A-I-Net STP-1	238081000 Capability Code 238043098	Not Applicable	NID = 238 Far End PCs: 238043006 238043007 238043008 238080000 238082000 238083000 238084000 238085000

Table 3-C. Example Point Code Information for ISUP Signaling (Contd)

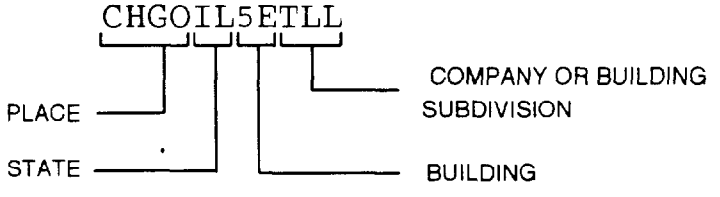
Signaling Point	Local PC	PCs in SS7 Trunk Translations	PCs in CNI Data Base
A-I-Net® STP-2	238082000 Capability Code: 238235099	Not Applicable	NID = 238 Far End PCs: 238235002 238083000 238235001 238084000 238080000 238085000 238081000 238043007
A-I-Net STP-3	238083000 Capability Code: 238235099	Not Applicable	NID = 238 Far End PCs: 238235002 238082000 238235001 238084000 238080000 238085000 238081000 238043007
A-I-Net STP-4	238084000 Capability Code: 238155097	Not Applicable	NID = 238 Far End PCs: 238080000 238083000 238081000 238085000 238082000
A-I-Net STP-5	238085000 Capability Code: 238155097	Not Applicable	NID = 238 Far End PCs: 238080000 238083000 238081000 238084000 238082000

4. *Common Language*® Location Identification Code Assignments

Definition and Use in SS7 Network

4.01 The CLLI codes are similar to Point Codes in that they are used as a means to uniquely identify switches, STPs, and SCPs in the network. However, unlike Point Codes, CLLI codes are not used for routing signaling messages. Instead, they provide a mnemonic identification of switches and signaling points that is particularly useful in reports and in trunk diagnostics. For an explanation of the CLLI code role in Circuit Validation Tests, refer to Chapter 6, "Circuit Validation Test".

4.02 Each CLLI code is assigned by the network administrator and consists of an 11-character field. The character field is divided into four subfields as shown below. The first four characters represent the city or place, the next two characters identify the state, the next two characters represent the building identifier, and the last three characters represent the company or building subdivision. The Place and State must be alphabetic while the Building and Subdivision can be alphanumeric. The CLLI code format is described in greater detail in 795-100-100, *CLLI Code Description.*



4.03 The CLLI code field must be populated; companies that do not usually use the CLLI code concept must choose a reasonable 11-character value for the field.

4.04 The term near-end CLLI code is synonymous with local CLLI code. Likewise, the term far-end CLLI code is synonymous with far CLLI code.

Sources of CLLI Code Information

4.05 For the 4ESS switch (and optionally for the 5ESS switch), the far-end CLLI code for trunks is stored in translation structures as part of the Circuit Identification Number (CIN). The CIN of an SS7 trunk circuit is verified as part of the ISUP circuit validation test.

4.06 The 1A ESS switch does not store the far-end CLLI code for trunks, but stores the local CLLI code in parameters.

4.07 The CNI data bases for the Lucent Technologies switches and the *A-I-Net* products STP require that near-end and far-end CLLI code information be populated for SS7 signaling links. Consistent representation of CLLI codes between the *A-I-Net* products STP and Lucent Technologies switch should be manually verified at both ends.

4.08 When populating CLLI code data, refer to Table 3-A for a summary of the recent changes.

Requirements for Populating CLLI Code Values

4.09 In addition to adhering to the format conventions specified for the CLLI code, the CLLI code that a given switch, STP, or SCP uses to identify itself should agree with the CLLI code that other signaling points in the network use to reference a particular switch, STP, or SCP. Changes to CLLI codes should not be made arbitrarily.

4.10 The CLLI codes must always be the CLLI code of the actual network element (switch, STP, or SCP) and not the CLLI code of other elements in the network (for example, Point of Presence).

Special Considerations

A. CLLI Code Assignments Relationship to CIN

4.11 A 4ESS switch trunk group, which consists of all the trunks between the 4ESS switch and a connecting switch, is defined by its CIN. The CIN in turn is based on the CLLI codes of the two connecting switches.

⇒ NOTE:
Note that there is only one Point Code allowed for a CIN. Multiple CLLI codes for a subdivision of trunks to the same Point Code cause recent change failures when building trunk subgroups.

B. Use in Circuit Validation Test

4.12 A 5ESS switch SS7 trunk group must specify the near-end CLLI code in populating Recent Change View 5.1; however, if Circuit Validation Tests are to be run ("**TRANS TEST**" = **Y**), then the far-end CLLI code must also be populated.

5. Link and Linkset Data

5.01 An SLK is a 56-kbps data link that connects two signaling points in an SS7 network for the purpose of SS7 signaling.

5.02 Because ISUP signaling messages are routed from a switch over an SLK to an STP, then from the STP over another SLK to another switch or STP, link information must be defined in the switches and STP's data bases. Successful routing and link operation require that link data between the switch and STP agree. Specifically, data consistency in eight data elements is required:

(1) **Linkset and Combined Linkset**—As signaling Linkset (LS) consists of all SS7 SLKs between two particular signaling points. For example, all SLKs between a switch and an STP are assigned a single LS. The LS is an arbitrary unique number at the signaling point, but not unique in the network.

The term Combined Linkset (CLS) refers to all the SS7 SLKs from a switch to the local pair of STPs or all the SS7 SLKs from an STP to another pair of STPs. All the signaling links from a switch to the local STP must have the same CLS value. *A-I-Net* products STP and combined linkset are not explicitly defined (they are implied in the routing data). The CLS value is unique to a signaling point, but is not unique in the network.

The 1A ESS switch, 4ESS switch, and 5ESS switch use a numerical value in the range of **1-255** to identify LSs and the CLS. The *A-I-Net* products STP, on the other hand, uses a **2-6** code consisting of two alpha and six numeric characters to identify the LS. Refer to 270-750-406, *A-I-Net Signaling Transfer Point, Data Base Administration Manual*, for additional information about the **2-6** code, and Table 3-D.

(2) **Point Codes**—The ANSI Point Codes are used to define the signaling points at the near-end and far-end of each SLK. The far-end Point Codes must agree with the locally specified values. For the specific requirements, refer to the "Point Code Assignments" in this chapter.

(3) **CLLI Codes**—Similar to Point Codes, CLLI codes are mnemonic identifiers of the signaling points at the ends of an SLK. The far-end CLLI codes must agree with the locally specified values. For the specific requirements, refer to the "CLLI Code Assignments" in this chapter.

(4) **Signaling Link Code (SLC)**—The signaling link code is a numeric value that a signaling point assigns each SLK within an SS7 linkset. Link information resides in each CNI data base and in the *A-I-Net* products STP data base.

Each SLK has a unique SLC within its linkset, while the SLC value assigned to the SLK at the near-end switch must agree with the SLC value assigned at the far-end STP. The identification of the linkset is different.

(5) **Link Type**—Link type defines which of the valid types of SLKs is used between the near-end and far-end entities.

(6) **Link Speed**—Link speed identifies the rate at which signaling messages are sent over the SLK. CNI support 56 kbps for SS7 signaling.

(7) **Encryption**—This option identifies whether or not the SLK encrypts (codes) signaling messages. A special link interface pack is required. However, the LEC network does not use this feature. Therefore, the encryption field should be set to a nonencrypted value (refer to Table 3-D).

(8) **STP Even/Odd Indications**—For 1A ESS and 5ESS switches, "**even**" or "**odd**" is selected as an arbitrary assignment with one restriction: all links to the STP must have the same designation point. That is, all SLKs to an STP must be "**even**" while all SLKs to its mate must be "**odd**".

The 4ESS switch, however, internally makes the "**even/odd**" association based on the value of the cluster field of the STPs. This implies that the STPs adjacent to the 4ESS switch must have "**even**" or "**odd**" cluster assignments.

5.03 Valid LEC values for the Linkset/Combination Linkset, SLC, Link Type, Link Speed, and Encryption are shown in Table 3-D.

Table 3-D. Link/Linkset Data

Data Item	*A-I-Net*® STP	5ESS® Switch	1A ESS™ Switch	4ESS™ Switch
Linkset Combined Linkset	2-6 Code	1-511 0-511	1-255	1-255
Signaling Link Code (LS Member)	0-15	0-15	0-15	0-15
Link Type (refer to Table 3-E)	A,B,C,D,E	A,E	A,E	A,E
Link Speed	56000	560	56000	56000
Encryption	NO	NOTENC	NO	NO

Note:
For the 1A ESS switch, link speed, link type, and encryption fields are initially defaulted to the list in the above table.

A-I-Net products STP uses **"LS Member"** as the term for SLC.

Link Type Value Definition

5.04 The link type field should be populated as follows on the types of signaling points at both ends of the link as shown in Table 3-E.

Table 3-E. Link Type to Signaling Point

Signaling Points at Each End	Link Type
A switch and a local STP	A
An STP and an SCP	A
A Local STP and a Local STP (Nonmated)	B
Mated STPs	C
A Local STP and Regional STP	D
Gateway STP to Gateway STP	D
A switch and a nonlocal STP	E

5.05 Activation of an SLK verifies the SLC, Origination Point Code, Destination Point Code, Link Speed, and Encryption. It does *not* verify the CLLI code or Link Type.

5.06 Figure 3-2 shows some of the link data required in the *A-I-Net* products STPs and Lucent Technologies switches. The network shown in Figure 3-1 is used as an example. The remaining data is entered in a like manner.

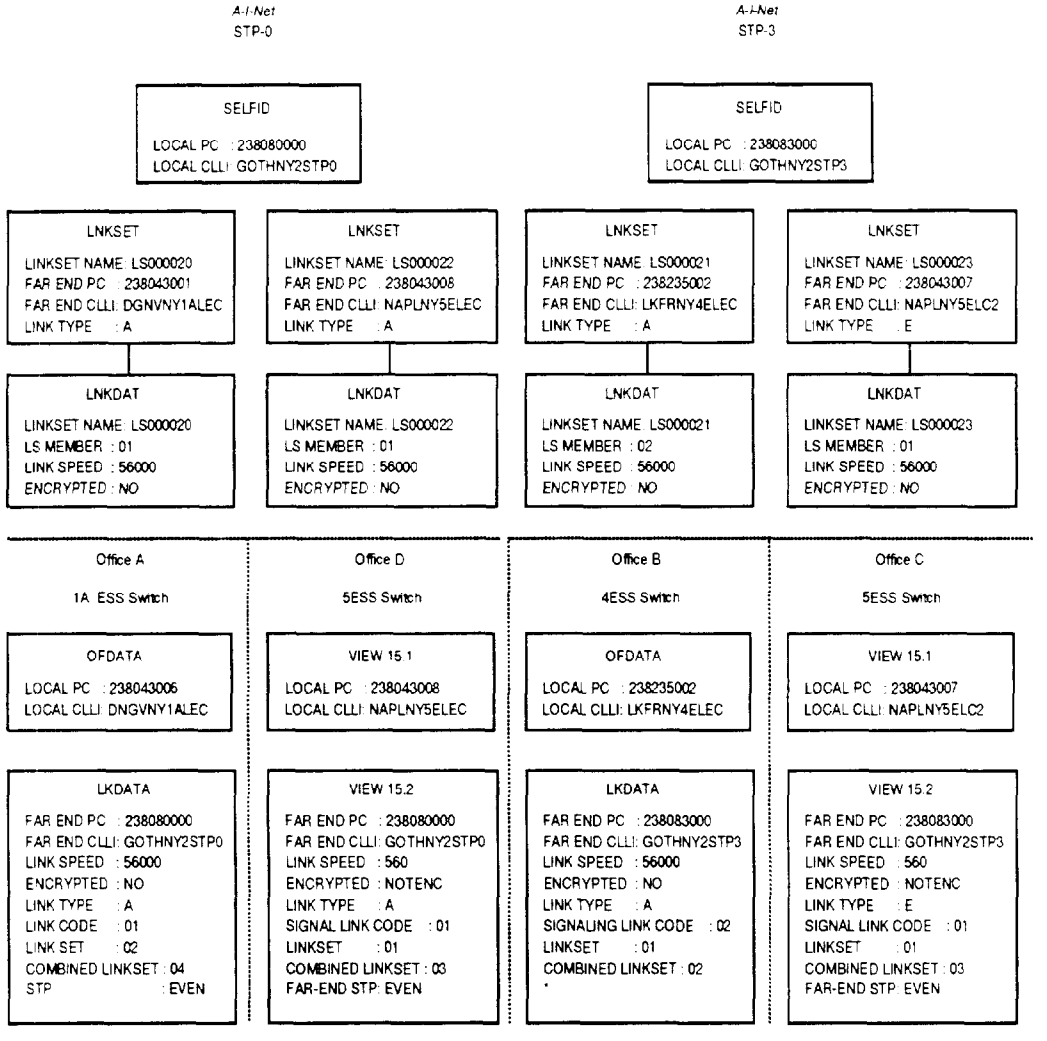


Figure 3-2. Example For Populating Link Node Data

6. Cluster Data

Definition and Use in the SS7 Network

6.01 The signaling message routing capability of SS7 requires that cluster information be populated in the CNI data base for each cluster of (destination) signaling points in a given LEC network. It is this cluster data that provides the broad definition of how the network is configured to the CNI.

6.02 Specific to ISUP functionality, cluster data (the middle 3-digit subfield of the Point Code) must exist for each of the switches to which ISUP messages are routed, as well as for the local STPs that act as the transfer points for the messages.

6.03 The local CNI uses the cluster information to verify that ISUP messages are destined for a valid cluster and to select the appropriate outgoing linkset. The ISUP does not require knowledge of capability codes, nonlocal STPs, or STP clusters.

6.04 The *A-I-Net* products STP also uses comparable cluster information to transfer the signaling messages toward their destination; however, the *A-I-Net* products STP data base is populated with the entire 9-digit Point Code field.

Sources of Cluster Data

6.05 Each CNI has a function or view that contains cluster information. When populating CNI cluster routing data, refer to Table 3-B for a summary of recent changes.

Switch Requirements for Populating Cluster Data

6.06 There are several considerations in assigning cluster values for ISUP signaling:

(1) Cluster fields must be populated for each local STP. This cluster value must agree with the cluster subfield within the far-end STP's *own* local Point Code.

(2) A cluster field should be populated for the local switch.

(3) Cluster fields must be populated for each switch where ISUP messages are to be routed.

(4) The cluster value of a far-end switch is stored both in CNI data and as a part of the far end PC in the trunk translation data structures. These two cluster fields must be the same for a given far-end switch. This Point Code value must also agree with the far-end switch's *own* local Point Code.

NOTE:
Cluster tables are populated only once for a unique cluster value. If two far-end switches are located in the same cluster (the cluster values are equal), only one view/function must be populated.

6.07 Figures 3-3 and 3-4 show the cluster information required in the switches of the example network shown earlier in Figure 3-1.

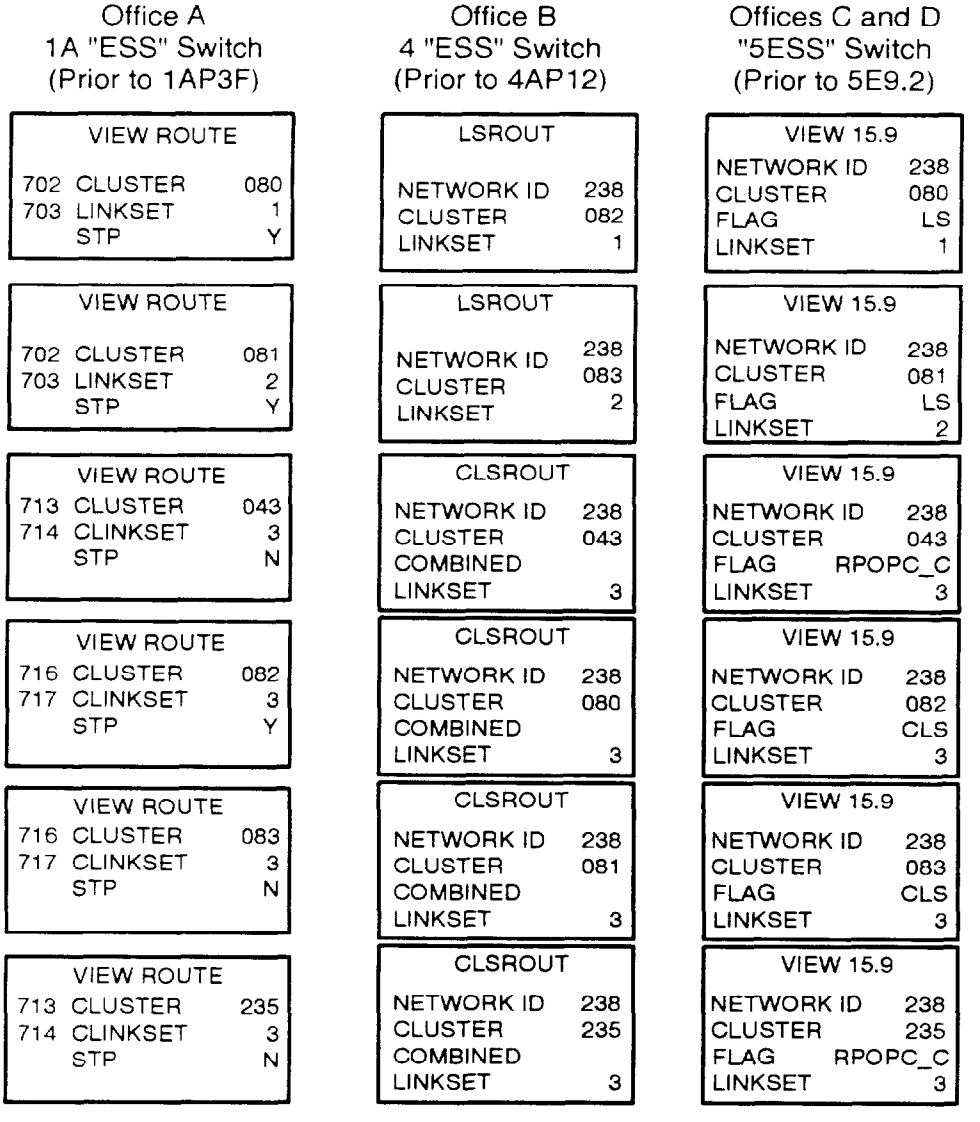


Figure 3-3. Example For Populating Switch Cluster Data (Without ALSR and E Links)

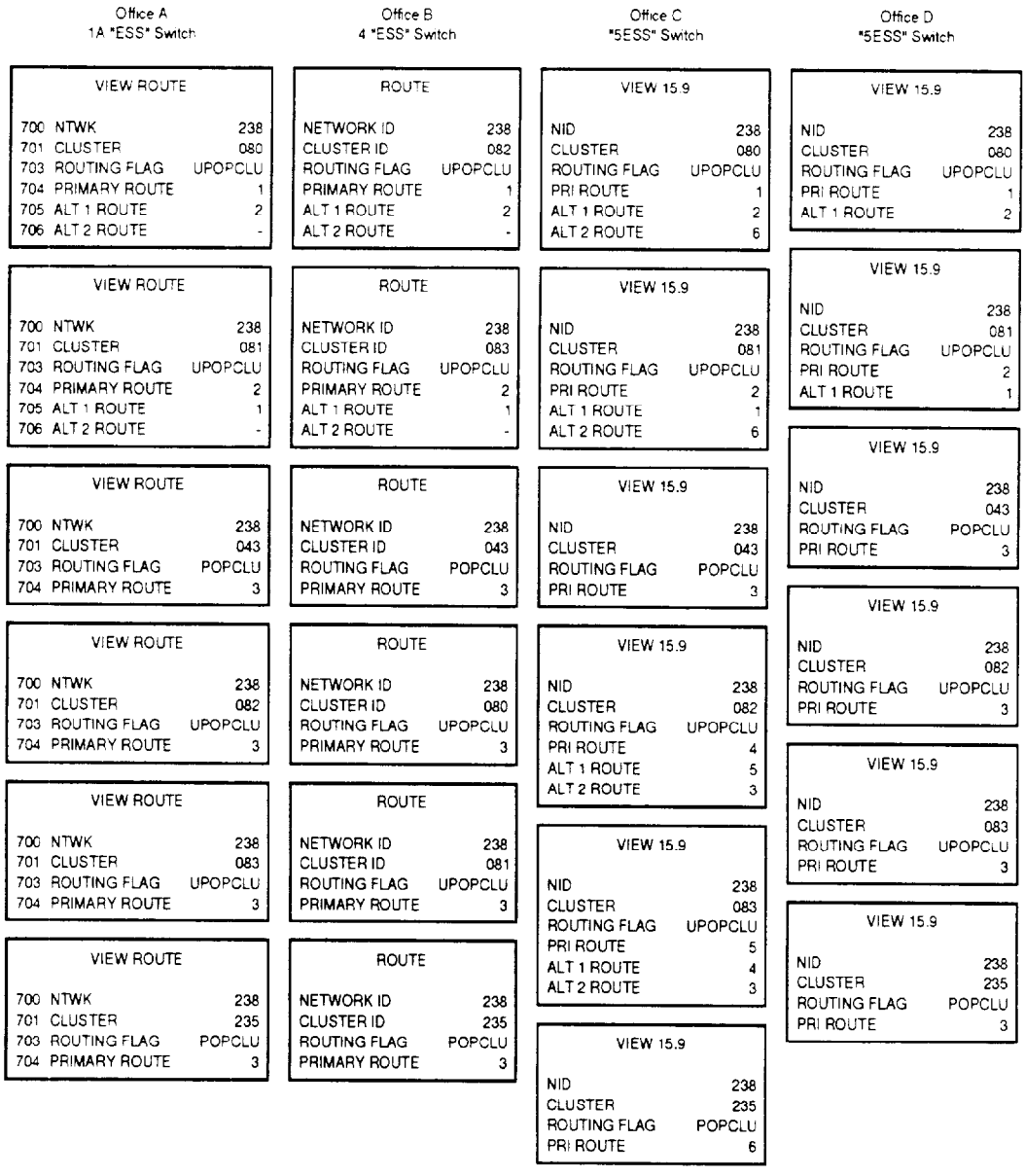


Figure 3-4. Example For Populating Switch Cluster Data (With ALSR and E Links)

A-I-Net Products STP Requirements for Populating Cluster Data

6.08 In the *A-I-Net* products STP, the cluster data (called the cluster routing data) actually consists of a list of PCs and their associated linksets and relative costs. Each PC represents either a local switch, local SCP, another STP, or a remote cluster.

6.09 In order for the *A-I-Net* products STP to route signaling messages to a particular switch, SCP, STP, or remote cluster under both normal and failure conditions, the linkset and cost parameters are required. An alternate route may be specified by populating a particular PC more than once with different linkset and cost parameters.

⇒ NOTE:
When creating the cluster routing data, it is not necessary to specify the C-linkset as an alternate route; this is automatic. However, a primary LS for the mate STP must be provided.

A combined linkset is implied by two routes to the same cluster with the same cost.

6.10 The cluster routing data is populated in the ordered route table via the "**ordrte**" recent change function. The linkset name must be specified using the "**2-6**" code. The valid range for the cost is **0** to **99**. An example of this data for the LEC network in Figure 3-1 is shown in Table 3-F.

Table 3-F. Example For Populating *A-I-Net* Products STP Cluster Routing Data

A-I-Net® **STP0 and** *A-I-Net* **STP1**			***A-I-Net* STP2 and** *A-I-Net* **STP3**			***A-I-Net* STP4 and** *A-I-Net* **STP5**		
Point Code	Link Set Name	Cost	Point Code	Link Set Name	Cost	Point Code	Link Set Name	Cost
238043006	LS000020	1	238080000	LS000230	1	238080000	LS000250	1
238043007	LS000021	1	238081000	LS000231	1	238081000	LS000251	1
238043008	LS000022	1	238084000	LS000240	1	238082000	LS000252	1
238082000	LS000230	1	238085000	LS000241	1	238083000	LS000253	1
238083000	LS000231	1	238043006	LS000230	1	238043000	LS000250	1
238084000	LS000240	1	238043006	LS000031	1	238043000	LS000251	1
238085000	LS000241	1	238043007	LS000230	1	238235000	LS000252	1
238235000	LS000230	1	238043007	LS000231	1	238235000	LS000253	1
238235000	LS000231	1	238043008	LS000230	1			
238155000	LS000240	1	238043008	LS000231	1			
238155000	LS000241	1	238043098	LS000230	1			
			238043098	LS000231	1			
			238235001	LS000020	1			
			238235002	LS000021	1			
			238155000	LS000240	1			
			238155000	LS000241	1			
(*)	LS000001	1	(*)	LS000001	1	(*)	LS000001	1

* For each STP, an entry must be made with the Point Code of the mate.

Special Considerations

6.11 The linkset field in the cluster data function needs to be consistent with other populated link data (refer to "Link and Linkset Data" in this chapter).

6.12 In switches, the "Linkset" field for the local STP clusters should be populated with the "Linkset" value used in the Link Node view/function for the SLKs to each STP. For all other clusters (for example, switch clusters), the "Linkset" field should be populated with the "Combined Linkset" value used in the Link Node view/function.

6.13 In *A-I-Net* products STPs, the "Linkset" field should be specified with the "**2-6** code" for the appropriate LS to route to the intended cluster/destination.

7. Miscellaneous Consistency Considerations

Protocol Timer and Parameter Settings

7.01 Recent change modifications (beginning with 5E9, 4AP12, and 1AP3F) to CNI timer and parameter settings should be made with caution. Changes to these values in translation structures can have significant impact on SS7 performance. This affects both STPs and other switches in the network. Adherence to the timer and parameter requirements specified in TR-NWT-000246, *Bell Communication Research Specification of Signaling System Number 7*, is recommended.

7.02 A summary of the default values for CNI timer and parameter settings is provided in Tables 3-G and 3-H. (Refer to Chapter 4 for information concerning NIDATA10, the audit which checks this data.)

7.03 The information concerning protocol timer and parameter settings, contained herein, may be found in the following documents:

Switch	Title
1A ESS	*TG-1A, 1A ESS Switch Translation Guide, Division 15*
	231-368-020, *1A ESS Switch, Attached Processor System/f1, Vol 1, Chapter 13*
5ESS	*TG-5, 5ESS Switch Translation Guide,* Division 9
4ESS	*TG-4, 4ESS Switch Translation Guide,* Division 12

Table 3-G. Lucent Technologies Recommended LEC Timer Settings

Timer	Description	Setting (Seconds)
Q703-T1	Aligned/Ready condition	13.0
Q703-T2	Out-of-alignment status	11.5
Q703-T3	Aligned condition	11.5
Q703-T4N	Normal proving period	2.3
Q703-T4E	Emergency proving period	0.6
Q703-T5	Busy status transmission	0.08
Q703-T6	Supervision of busy state	3.0
Q703-T7	Excessive delay of acknowledgement	1.0
TS	Signaling Unit Error Rate Monitor's Threshold (SUERM)*	64 (errors/sec.)
Q704-T1	Transmission delay following changeover	1.0
Q704-T2	Changeover acknowledgement	1.0
Q704-T3	Transmission delay following change back	1.0
Q704-T4	First attempt Change Back Acknowledgement (CBA)	1.0
Q704-T5	Subsequent attempts CBA	1.0
Q704-T6	Controlled rerouting transmission delay	1.0
Q704-T8	Inhibit Sending Transfer Prohibited (TFP)†	1.0
Q704-T10	Wait to repeat Signaling Route Set Test (SRST) message	30.0
Q704-T11	Transfer Restricted (TFR)†	30.0
Q704-T12	Uninhibit acknowledgement	1.0
Q704-T13	Forced uninhibit acknowledgement	1.0
Q704-T14	Inhibit acknowledgement	3.0
Q704-T15	Transfer-controlled update	3.0
Q704-T16	Signaling-route-set congestion	1.4

* This is not a timer, but a timed-event counter.

† This timer is used in *A-I-Net*® products STPs only.

Note:
Many of these timers may be set for one link, one linkset, or all linksets (office level).

Table 3-H. Lucent Technologies Recommended LEC Timer Settings

Timer	Description	Setting (Seconds)
Q704-T17	Restart of initial alignment	1.0
Q704-T18	Transfer Cluster Restricted (TCR)*	30.0
Q704-T19	Timeout for attempting link activation	480.0
Q704-T20	Waiting to repeat local inhibit test	120.0
Q704-T21	Waiting to repeat remote inhibit test	120.0
Q707-T1	Supervision timer for signaling link test acknowledge message	10.0 (≥ Q704-T6)
Q707-T2	Sending Signaling test message interval	30.0
Q714-TSST	Delay between requests for subsystem status	30.0
Q714-TSOG	Waiting for grant for subsystem to go Out-of-Service (OOS)	30.0
Q714-TIGSST	Delay for subsystem between receiving grant for OOS and actually going OOS	30.0
Q714-TSRT	Interval between requests for subsystem routing status information	30.0

* This timer is used in *A-I-Net*® products STPs only.

Note:
These timers may be set on the basis of one or more of the following: one link, one linkset, or all linksets (office level).

Table 3-I. Lucent Technologies Linkset Threshold Settings (CNI Congestion)

Threshold*	Description	Setting (Bytes)
cc_abt1†	Link Transmit Buffer Control-Abatement Threshold Level 1	820
cc_ths1†	Link Transmit Buffer Control-Onset Threshold Level 1	3072
cc_dis1†	Link Transmit Buffer Control-Discard Threshold Level 1	6042
cc_abt2†	Link Transmit Buffer Control-Abatement Threshold Level 2	7680
cc_ths2†	Link Transmit Buffer Control-Onset Threshold Level 2	8295
cc_dis2†	Link Transmit Buffer Control-Discard Threshold Level 2	10855
cc_abt3†	Link Transmit Buffer Control-Abatement Threshold Level 3	10855
cc_ths3†	Link Transmit Buffer Control-Onset Threshold Level 3	10956
cc_dis3†	Link Transmit Buffer Control-Discard Threshold Level 3	11571

* These thresholds may be set for one linkset or all linksets (office level).

† The congestion threshold values (for ABT_, THS_, DIS_) are interdependent. Changes to one **MUST** be coordinated with the values, or changes to the values, of the others in the same level.

Switch Routing Limit Table

7.04 Five parameters (and values) set the limits for both Intranetwork and Internetwork SPs. The values are determined by the CNI; however, the values are set by the SP application and cannot be changed. Shown in Table 3-I are the five values that are provided for customer awareness.

Table 3-J. Intranetwork and Internetwork Values

# Define	1A ESS™	4ESS™	5ESS®	*A-I-Net®* STP
NDIRMAX	24	24	24	32
LPCLUMAX	128	128	128	128
NPCLUMAX	384	384	384	512
LPCMIN	231	231	231	2048
NPCMIN	2769	2769	2769	4096

7.05 The limits are defined as:

(1) Maximum Network (**NDIRMAX**)—The maximum number of Network Identifications (other than the local network) that can be defined on a per switch basis.

(2) Local Populated Cluster Maximum (**LPCLUMAX**)—The maximum number of clusters that can be assigned to remote routing (RPOPC) in the local network.

(3) Nonlocal Populated Cluster Maximum (**NPCLUMAX**)—The maximum number of clusters that can be assigned to remote routing (RPOPC) in all networks other than the local network (switch).

(4) Local Abnormal Members (**LPCMIN**)—The minimum number of members whose routing status can be concurrently maintained for the local network.

(5) Nonlocal Abnormal Members (**NPCMIN**)—The minimum number of members whose routing status can be concurrently maintained for all networks.

8. Trunk Circuit Identification Code Assignments

TCIC Assignments —Definition and Use in the SS7 Network

8.01 A Trunk Circuit Identification Code (TCIC) is a numeric value assigned to an SS7 trunk. Each trunk is uniquely identified by its TCIC and Point Code combination (Originating and Destination). In order for connecting switches to establish a voice path or run end-to-end trunk tests, it is critical that agreement exists on how the trunk is to be identified. The TCIC assignment must be identical in both offices for a given trunk circuit.

8.02 It is also important to note that TCIC assignment indirectly affects distribution of signaling message traffic over the SLKs. This is because the TCIC assignment determines (via an algorithm) the value in the Signaling Link Select (SLS) field in the Message Transfer Part (MTP) routing label. The SLS field is used for determining load sharing between the signaling links in a linkset.

8.03 The 5ESS switch uses the term CLCI TRK ID code for trunk circuit identification code.

Sources of Trunk Circuit Identification Code Information

8.04 The TCIC information is stored in trunk translation structures on a per-trunk basis. When populating TCIC code data, refer to Table 3-A for a summary of the recent changes.

Requirements for Trunk Circuit Identification Code Assignments

A. Requirements When Connecting Switches Are 1A ESS™ and/or 5ESS® Switches

8.05 Initially, TCIC values for the same trunk group should be assigned *sequentially*. The benefits of *sequential assignments* results in fewer group blocking messages in the event of a carrier failure. For example, if circuits need to be blocked, only one group blocking message is needed to block a sequential range of TCIC. Sequential assignment also results in a uniform distribution of Signaling Link Selector (SLS) values within a trunk group.

8.06 In addition, for the 1A ESS switch, sequential assignment of TCICs can reduce memory usage. An entire TCIC block is allocated once a single TCIC is specified within a block of 256 TCICs.

For these reasons, a series of four steps are recommended when assigning circuit identification code values:

(1) Identify the SS7 trunks which are on a Carrier Group Alarm (Software or Hardware).

(2) Within each Carrier Group Alarm, group the trunks by Destination Point Code (DPC).

(3) For each trunk group within a DPC, assign sequential TCIC values for one Carrier Group at a time. The TCIC values are unique between connecting switches.

(4) Assign TCICs sequentially to any remaining trunks, one DPC at a time.

B. Requirements When One Connecting Switch Is a 4ESS™ Switch

8.07 The 4ESS switch uses the Traffic Number to define the TCIC value. Offices connecting to a 4ESS switch must assign TCIC values to agree with the 4ESS switch assignment of traffic numbers.

Special Considerations

8.08 Do not leave gaps in TCIC assignments (that is, unassigned TCICs) in anticipation of facility or trunk group growth.

8.09 When assigning TCICs, consideration must be given to the range of values allowed by each switching system as shown in Table 3-J.

Table 3-K. TCIC Valid Code Ranges

System	Valid Trunk Circuit Identification Code Range
1A ESS™ switch	0 - 16383
4ESS™ switch	0 - 9999
5ESS® switch	0 - 9999

NOTE:
For the 4ESS switch, all TCICs in the range of **0 - 9999** are available; however, there is a convention used by the 4ESS switch Administrators that does not use TCICs ending in **97 to 100**. There is nothing in the software or rules that enforces this convention.

9. Trunk Provisioning

9.01 To provision SS7 Integrated Services Digital Network User Part (ISUP) trunks the switch must first have an operational CNI ring. In addition, CNI routing data must be entered for each Network Identifier and cluster of a switch to which the SS7 ISUP trunks are provisioned.

NOTE:
Although provisioning is separated in this section by function, the reader must not fall into the trap of addressing only one or two of the items listed below. These functions must all be addressed when provisioning.

(a) Basic Trunk Signaling

(b) Glare

(c) Voice Path Assurance

(d) VPA/Continuity Check Circuits

(e) Trunk Hunting

(f) Circuit Query

(g) Trunk Translation Test/Audit.

Basic Trunk Signaling

9.02 The sections that follow identify the basic trunk signaling data that must be addressed for each Lucent Technologies switching product.

A. 1A ESS Switch

Recent change message **RC:TG** is used to change trunk group information. Fields of particular importance for SS7 ISUP trunks are identified in Table 3-K.

Table 3-L. Trunk Group Recent Change Messages

Keyword	Description
PC	This field identifies the PC at the far-end of the trunk.
TYP	This field identifies the trunk type. Allowable trunk types for SS7 are: 1, 2, 10, and 15.
TLSALL	This field indicates whether an inband tone/announcement (T/A) or an SS7 release message is to be returned for calls using SS7 signaling all the way. It is used for terminating Local Access and Transport Area (LATA) subtending screening failures. If set, the inband T/A is provided; if not set, an SS7 release message is returned.
TLSNOT	This field indicates whether an inband T/A or an SS7 release message is to be returned for calls not using SS7 signaling all the way. It is used for terminating LATA subtending screening failures. If set, the inband T/A is provided; if not set, an SS7 release message is returned.

9.03 Recent change message **RC:TGMEM** is used to change trunk member information as shown in Table 3-L. Fields of particular importance for SS7 ISUP trunks include:

Table 3-M. Trunk Member Recent Change Messages

Keyword	Description
PC	This field identifies the PC at the far-end of the trunk.
CIC	This field identifies the SS7 ISUP TCIC uniquely assigned to each trunk member for a particular Destination Point Code (DPC).

B. 4ESS Switch

9.04 Recent change message **RC:TSG** is used to change trunk subgroup information. Fields of particular importance for SS7 ISUP trunks are identified in Table 3-M.

Table 3-N. Trunk Subgroup Recent Change Messages

Keyword	Description
PCF	This field specifies the Destination Point Code format. Recommended format is "ANSI" for LEC switches.
DPC	This field specifies the Destination Point Code of the far-end switch.
TSG	This field identifies the particular trunk subgroup. It is comprised of the TCIC and *Common Language* CLLI code associated with the far-end switch.
TOT	This field specifies the type of SS7 trunk defined. Acceptable values include "ETC" (meaning End Office or Tandem Office Connecting trunk) or "OCC" (meaning Other Carrier Connecting trunk).
ISC	This field identifies the Incoming Signaling Characteristics. For SS7 2-way and 1-way incoming trunks, it should be set to "ISUP".
OSC	This field identifies the Outgoing Signaling Characteristics. For SS7 2-way and 1-way outgoing trunks, it should be set to "ISUP".

9.05 Recent change message **RC:TRK** is used to add/change individual trunk characteristics. A field of particular importance for SS7 ISUP trunks is identified in Table 3-N.

Table 3-O. Individual Trunk Recent Change Messages

Keyword	Description
FTFN	This field specifies the First Traffic Number of the far-end switch. The TCIC assigned to the same trunk at the far-end must be the same as the traffic number at the switch.

C. 5ESS Switch

9.06 In the 5ESS switch, trunk group view 5.1 is used for recent change of trunk group information as shown in Table 3-O. The TCIC assigned to the same trunk at the far-end must be the same as the traffic number at the switch.

Table 3-P. Recent Changes for Trunk Group View 5.1

Field	Description
INPLS	This field indicates the incoming address signal mode. For SS7 ISUP 2-way trunk groups and 1-way incoming trunk groups, this field should be set to "ISUP7". For 1-way outgoing trunk groups, this field should be set to "NONE".
OUTPLS	This field indicates the outgoing address signal mode. For SS7 ISUP 2-way trunk groups and 1-way outgoing trunk groups, this field should be set to "ISUP7". For 1-way incoming trunk groups, this field should be set to "NONE".
NEAR CLLI	This field is the near-end CLLI code of the trunk group. This field should be populated with the same value assigned as field **LOCAL CLLI** in Office Identification recent change view 15.1.
DEST PT CODE	This field identifies the PC of the far-end switch. For inter-module trunks, refer to 235-190-120, ***5ESS*** *Switch Common Channel Signaling Service Features*, for more information on populating this field.
ORIG PT CODE	This field is the local switch's PC. This field is initially populated automatically from the **LOCAL POINT CODE** field in Office Identification recent change view 15.1.
CCS7 TYPE	This field should be set to "RBOC" (generic software release 5E6), "BELLCORE" (5E7 and later), and indicating a LEC switch.
FAR CLLI	This field identifies the far-end CLLI code of the trunk group. This field must be populated correctly for the **AUD:CCSXLATE** circuit audit to pass.
TRANS TEST	This field may be set to "**Y**" or "**N**". If set to "**Y**", this indicates that the **CVTs** are to be run, then the Far-End CLLI code must be populated.

9.07 In the 5ESS switch, trunk member view 5.5 is used for recent change trunk member information for a single trunk or a range of trunks in a trunk group. Particular fields of importance are shown in Table 3-P.

Table 3-Q. Recent Changes for Trunk Member View 5.5

Field	Description
CLCI TRK ID	This field contains the SS7 ISUP TCIC. The TCIC must be unique for each trunk group member to a particular destination Point Code.
IN START DIAL	This field indicates the incoming start signal. For SS7 ISUP trunks, this field should be set to "NON"E or left blank (defaulting to "NONE").
OUT START DIAL	This field indicates the outgoing signal type. For SS7 ISUP trunks, this field should be set to "NONE" or left blank (defaulting to "NONE").

Glare

9.08 Glare is a condition that occurs when two connecting switches hunt and seize the same 2-way trunk simultaneously. In the event a glare condition occurs, both switches must know which one has control over the trunk. The glare parameters in the switches make this determination.

9.09 The glare parameters to be populated in the two switches should be coordinated. Previously, glare was normally resolved with the higher (numerical) Point Code switch controlling trunks with even trunk circuit identification codes (Odd/Even Rule). New additional options exist to control "all" or "none" of the trunk circuit identification codes. (Refer to the following paragraph and Tables 3Q and 3R).

9.10 Glare settings are made on a trunk group basis in the 5ESS switch and 1A ESS switch. They are made on a trunk subgroup basis in the 4ESS switch. Table 3-Q summarizes the necessary recent changes for populating glare data.

Table 3-R. Glare Data Recent Changes

Office Type	Function/ View	Keyword/ Field	Description
1A ESS™ Switch	RC:TG	GLRCTRL (SS7 Only)	This field indicates the all/none glare control indicator. If set, the office trunk group has control in glare situations. Otherwise, the office trunk group does not have control in glare situations.
	RC:TG	GLRIND (SS7 Only)	This field indicates the SS7 glare method to be used. If set, the office trunk group uses the All/None method of glare resolution. Otherwise, the Odd/Even method of resolution is used.
	RC:TG	GLRM (Non-SS7)	This field indicates the glare master control. In the event of glare, the far-end of the trunk is expected to yield and forward hunting does result.
4ESS™ Switch	RC:TSG	GLARE	This field specifies the glare control action for 2-way trunk subgroups. The data administrator must specify Odd, Even, All, or None.
5ESS® Switch (5E6)	5.1	GLARE ACTION	This field specifies the glare control action for 2-way trunks. Potential values include "Odd/Even", "allctrl", or "nonectrl", corresponding to Odd/Even, All, or None methods of glare resolution, respectively.

9.11 Requirements for treatment of glare are described in Bellcore's TR-NWT-000317, *Switching Systems Requirements for Call Control Using the Integrated Services Digital Network User Part.* To comply with glare control based on the "Odd/Even" or the "All or None" Rules, refer to Table 3-R.

9.12 For 1-way trunk groups, glare settings are not normally needed; however, refer to Chapter 6, "Circuit Validation Test", for additional information.

Table 3-S. Glare Control Input Requirements

Office Type (Generic)	Glare Control	Input Requirements
1A ESS™ Switch	Odd/Even	**GLRIND** = "N" (**GLRCNTL** is not input)
	All	**GLRIND** = "Y" and **GLRCNTL** = "Y"
	None	**GLRIND** = "Y" and **GLRCNTL** = "N"
4ESS™ Switch	Odd/Even	If the near-end PC is lower, set **GLARE** = "O". If the near-end PC is higher, set **GLARE** = "E".
	All	**GLARE** = "A"
	None	**GLARE** = "N"
5ESS® Switch	Odd/Even	**GLARE ACTION** = "ODDEVEN"
	All	**GLARE ACTION** = "ALLCTRL"
	None	**GLARE ACTION** = "NONECTRL"

NOTE:
In the 4ESS switch, the data administrator must specify whether the near-end PC is higher or lower than the far-end PC using ANSI standard PC format.

Voice Path Assurance

Definition and Use in the SS7 Network

9.13 Because SS7 does not signal through actual trunk circuits, Voice Path Assurance (VPA) tests are needed to ensure that transmission through the voice path is acceptable*. These tests, also called Continuity Checks, are initiated by the originating switch (which may be the local switch or a connecting switch) either manually or on a per-call basis. These tests may also be initiated via APT on an automated basis. This part provides the network administrator with the necessary information to provision a Lucent Technologies switch to perform VPA testing on a per-call basis.

9.14 Two data elements are associated with VPA: the VPA type and the VPA rate. The VPA type reflects the type of connecting (far-end) switch. The continuity tone frequency that is sent and detected is determined by the VPA type. Four-wire switches (for example, 4ESS switch or 5ESS switch) can detect a 2,010-Hz (± 8 Hz) tone and can send either a 1,780-Hz (± 30 Hz) or 2,010-Hz (± 8 Hz) tone as shown in Table 3-S.

9.15 Two-wire switches (for example, a 1A ESS switch or a 5ESS switch emulating a 2-wire switch) can send and receive both tones. Since LEC networks can be configured with both types of switches (2-wire and 4-wire), there are four possible VPA type combinations.

Table 3-T. VPA Test Frequencies for 2-Wire and 4-Wire Switches

Near-End Switch	Far-End Switch	
	2-Wire	4-Wire
2-Wire	2,010 Hz sent, 1,780 Hz returned	2,010 Hz sent, 1,780 Hz returned
4-Wire	1,780 Hz sent, 2,010 Hz returned	2,010 Hz sent, 2,010 Hz returned

9.16 The VPA rate reflects the percentage of time VPA tests are required on a per-call basis. Normally, an interoffice SS7 call sends an Initial Address Message (IAM) to the connecting switch announcing a new call is being attempted.

* Requirements for acceptable transmission are specified in TR-NWT-000317, *Switch System Requirements for Call Control Using the Integrated Services Digital Network—User Part (ISDN-UP)*, and TR-NWT-000246, *Bell Communications Research Specifications of Signaling System 7.*

An indicator (bits DC of the nature-of-connection indicators parameter) in this IAM message requests that the far-end switch perform a VPA test on the trunk facility before call setup to ensure it is suitable for voice transmission.

9.17 The continuity tests are handled by special VPA test circuits. Because the tests require an available VPA test circuit and the need for VPA tests is dependent on the type of trunk facility, each switch offers options for the VPA rate (these options are described later in this chapter). The VPA test is allowed 2 seconds to succeed; if the test does not pass within 2 seconds, time-out (failure) will occur.

9.18 The VPA test circuits must be engineered to handle the combined usage for outgoing and incoming VPA tests. Outgoing VPA tests are based on the VPA rate of the local switch; while incoming VPA tests are controlled by the connecting switch. Thus, the VPA rate also affects VPA test circuit usage in connecting switches.

1A ESS Switch/VPA Data Specifics

9.19 VPA data in the 1A ESS switch is populated on a Trunk Class Code (TCC) basis. Recent Change input message **RC:PSWD** is used to modify the TCC translator. The VPA data fields in the TCC translator are listed in Table 3-T.

Table 3-U. RC Messages for TCC and VPA Data

Field	Description
Continuity Checks Canceled	0 = All (1/1) calls have continuity check performed 1 = 1-out-of-8 calls have continuity check performed
Continuity Check Tone Frequency	0 = 2-wire far-end switch 1 = 4-wire far-end switch
Continuity Check Tone Level	LEVEL INSERTED CONNECTION LOSS 1 0.0 to 4.0 dB 2 4.1 to 8.6 dB (no high-loss trunking) 3 4.1 to 8.6 dB (high-loss trunking)

NOTE:
The Inserted Connection Loss (ICL) is the 1,004-Hz transducer loss of the circuit referenced to the nominal impedance of the switches (600 to 900 ohms) which the circuit interconnects. It reflects all of the gains and losses from the originating switch's outgoing appearance (through the incoming circuit) to the incoming appearance on the terminating switch in the nominal switch impedance.

4ESS Switch / VPA Data Specifics

9.20 The VPA type in the 4ESS switch is populated on the trunk subgroup and rated on a trunk member basis. Table 3-U lists the RC input messages and their corresponding fields used to populate VPA data.

Table 3-V. RC Messages for Populating VPA Data

Message	Keyword	Description
RC:TRK	VCR	This field specifies the **cancellation rate** of the VPA test. This is the percentage of time VPA tests are canceled (that is, not requested) on a per-call basis. Valid entries are 100, 87, 50, or 0.
RC:TSG	XCPA	This field corresponds to the transceiver pad adjustment. Valid entries are 0, 1, 2, or 3. The correct entry is determined by comparing the highest ICL value assigned to a trunk in the Trunk Subgroup. DIGIT ICL APPLICATION PAD 0 0 loss trunk 5 dB 1 0.1 to 0.8 loss 3.5 dB 2 0.9 to 1.7 loss 1.8 dB 3 1.8 to 4.1 loss 0 dB
RC:TSG	CCIS2WIRE	This field corresponds to whether the far-end switch is a 2-wire or 4-wire switch. If the far-end switch is 2-wire, set this field to "**Y**". If the far-end switch is 4-wire, set this field to "**N**".

5ESS Switch/VPA Data Specifics

9.21 The VPA data in the 5ESS switch is populated on the trunk group basis. Table 3-V lists the recent change messages and their corresponding fields for populating VPA data.

Table 3-W. RC Messages for Populating VPA Data

View	Field	Description
5.1	VPA RATE	This field gives the percentage of calls on which a VPA test should be run. Valid entries are 0, 12, 50, or 100.
5.1	VPA TYPE	5ESS® software can select either NOVPA, 4W4WL[0-3], 4W2WL[3-5], 2W4WL[0-3], or 2W2WL[3-5]. If the switch performs a VPA test, the first two characters describe the near-end switch's wire type (4-wire or 2-wire) and the next two characters describe the far-end switch's wire type (4-wire or 2-wire). The level chosen corresponds to the ICL range shown on the next table (Table 3-W).
14.1	TEST CODE	An automatic trunk test table number must be provisioned. The test table number should have this field set to "CONT" (the test code for continuity check). The automatic trunk test table number should be assigned to SS7 ISUP trunks using the trunk group view 5.1 field ATTN, thereby making the continuity check (or VPA test) the default trunk test for that trunk group.

9.22 Table 3-W shows the correspondence between the **ICL** value and level used in the **VPA** type field on the preceding page.

Table 3-X. Inserted Connection Loss

5ESS® Switch Type	Inserted Connection Loss Level	
4-Wire	0	0
	1	0.1 to 0.8
	2	0.9 to 1.7
	3	1.8 to 2.9
	4	0.0 to 4.0
	5	4.1 to 5.5 (no high-loss trunking)
	6	4.1 to 5.5 (high-loss trunking)
2-Wire Emulation	0	0
	1	0.1 to 0.8
	2	0.9 to 1.7
	3	1.8 to 2.9 (4-wire far end)
	3	0.0 to 4.0 (2-wire far end)
	4	4.1 to 5.5 (no high-loss trunking)
	5	4.1 to 5.5 (high-loss trunking)

Guidelines for Populating VPA Data

VPA Type

9.23 When the far-end switch is a 1A ESS switch, the VPA type must be 2-wire. When the far-end switch is a 4ESS switch, the VPA type must be 4-wire. Normally, 5ESS switches are treated as 4-wire, but may be designated as 2-wire for VPA purposes to aid in replacement of a 1A ESS switch with a 5ESS switch.

VPA Rate

9.24 To set specific VPA rates for SS7 trunk facilities, each switch must consider the trade-off between:

(1) The cost of the VPA test circuit and the additional time required for call setup

(2) The reliability objectives.

9.25 Table 3-X gives minimal VPA rate (or, in the case of the 4ESS switch, Cancellation Rate) guidelines based on the type of trunk facility.

Table 3-Y. Minimal VPA Rates

Trunk/Circuit Type	1A ESS™ Switch	4ESS™ Switch	5ESS® Switch
UNALARMED	1/1	0% (= 100% test rate)	100%
SOFTWARE CARRIER ALARMED	1/8	87% (= 12.5% TEST RATE)	–
HARDWARE CARRIER ALARMED — Analog switch or multiple spans w/o end-to-end alarms at switch	1/8	87% (= 12.5% TEST RATE)	12%
HARDWARE CARRIER ALARMED—Digital end-to-end alarms	–	87% (= 12.5% TEST RATE)	0%

NOTE:
These are minimum VPA guidelines. For other available VPA rates, check the appropriate translation guide. The rate must be consistent with the hardware equipped at each end of the trunk facility.

Special Circumstances

A. 1A ESS Switch

9.26 Office option **CCME** (Item 109 of 1A ESS 1500D form in TG1A) allows an outgoing call to proceed instead of being blocked if no outgoing VPA test circuit is available *and* if the VPA rate is set at 1/8. If the rate is 1/1, the call is blocked. Blocking will continue until a VPA test circuit is available. The setting of this option is an engineering consideration based on the quantity of VPA test circuits.

9.27 The 1A ESS switch separates incoming and outgoing VPA test circuits via fixed Route Indexes. Overflow could be used to allow incoming requests to use the outgoing Route Index. The use of separate trunk groups from each fixed route index is an engineering consideration based on the number of available VPA test circuits.

B. 5ESS Switch

9.28 The 5ESS switch encodes Inserted Connection Loss in the same recent change field as **VPA type** (RCV view 5.1).

9.29 A test table number must be assigned to each SS7 trunk group (RCV view 14.1) and its **TEST CODE** must be populated with **"CONT"**.

C. Office Replacement Impact on Trunk Testing

9.30 When an SS7 capable 1A ESS switch is replaced with a 5ESS switch, a consideration occurs with precutover testing of ISUP trunks between the replacement 5ESS switch and offices connecting to the 1A ESS switch being replaced. The problem concerns VPA testing and related craft activities both during precutover and at the time of cutover to the replacement 5ESS switch. This problem occurs because the 5ESS switch is a 4-wire switch while the 1A ESS switch is a 2-wire switch. The frequencies transmitted and received for VPA tests are different for 2-wire and 4-wire switches (refer to Table 3-S).

9.31 Currently, when an ISUP trunk is tested during precutover, recent change activity is required at the far-end switch to indicate that a 4-wire, rather than a 2-wire, VPA test is to be performed. Once the testing is completed, and the trunk rehomed back to the 1A ESS switch, these recent changes must be reversed. At the time of cutover to the replacement 5ESS switch, coordinated recent changes must be made at each of the far-end switches whose trunks are being moved from the 1A ESS switch to the replacement 5ESS switch to again indicate that 4-wire VPA testing is to be done.

9.32 The solution to this problem is to have the replacement 5ESS switch emulate a 2-wire VPA test (2-wire emulation) in terms of the frequencies transmitted and received. For this purpose, switch development has been performed on generics 5E5 and later to allow the 5ESS switch to emulate a 2-wire switch (refer to Chapter 7, "Miscellaneous Engineering Considerations," for additional information).

This development is reflected in the new VPA types **2W4WL[0-3]** and **2W2WL[3-5]**.

9.33 Setting the VPA type to one of these allows precutover 2-wire ISUP trunk testing to be performed without requiring recent changes to the VPA data at far-end switches. Similarly, no recent changes to the VPA data at far-end switches are mandated at the time of cutover to the replacement 5ESS switch. Once the cutover is complete, trunk data at the replacement 5ESS switch and the far-end switches can be updated, on a gradual basis, to indicate that 4-wire VPA testing is to be done. Alternatively, the 2-wire VPA testing can be left in place. The choice between these two alternatives can be made on a per far-end switch basis.

VPA/Continuity Check Circuits

9.34 The VPA circuits (Table 3-Y), sometimes called Continuity Check circuits, must be engineered to handle the combined usage for outgoing and incoming VPA tests. Outgoing VPA tests are based on the VPA rate of the originating switch, while incoming VPA tests are controlled by the far-end switch's VPA rate. The VPA test is a per call test whose rate can be adjusted. Hence, the VPA rate also affects VPA test circuit usage in connecting switches.

Table 3-Z. Service Circuits Required for VPA Testing

Switch	Service Circuit
1A ESS™	Continuity Check Circuit SD-1A436, CPI 088 (2-wire) SD-1A453, CPI 203 (HILO 4-wire)
4ESS™	Continuity Check Transceiver SD-4A081 (CCT and looparound test units) SD-4A064 (SS7 CCT units)
5ESS®	Digital Service Unit (DSU)—Model 2 or LDSU Model 1 with TN1637 circuit pack

9.35 Engineering the appropriate quantity of VPA circuits depends on the quality of service each LEC is willing to provide to its customers. On the one hand, requiring a VPA test on every call ensures that the trunk transmission quality meets the minimum requirements, but also increases the call setup time and requires significantly more VPA circuits. On the other hand, performing a VPA test on one-out-of-every-eight calls reduces the quantity of VPA circuits needed, but also increases the probability that a call receives a trunk failing minimum transmission requirements. The ideal quantity is to be decided by each LEC data administrator. For guidelines in engineering the minimum number of VPA circuits, refer to the following documentation:

- 1A ESS—Central Office Equipment Engineering System (COEES) Index 60, Common Channel Signaling Number 7 Features
- 4ESS—234-060-210, *4ESS Switch Network Switching Engineering, Service and Miscellaneous Circuits*
- 5ESS—235-060-110, *5ESS Switch Engineering Procedures*

9.36 Once the initial quantity of VPA circuits has been determined, the network administrator must determine whether or not the quantity installed is sufficient for the VPA testing needs of the office.

Table 3-Z summarizes measurements to be used to determine if more VPA circuits are needed.

Table 3-AA. VPA Circuits Requirements

Office Type	Report	Field Name	Description
1A ESS™ Switch	H or C Traffic Schedule	TMC 2, EGO tg#	This traffic measurement count for the specified trunk group identifies the number of times a continuity check circuit is requested with no idle continuity check circuit available.
	H or C Traffic Schedule	TMC 0 EGO tg#	This traffic measurement count identifies the total amount of time that all continuity check circuits are in use.
4ESS™ Switch	Machine Service Report, Part 2 (MSR2)	ISUP XCVR	This measurement is the number of times that transceivers are *not* available for continuity tests.
5ESS[3] Switch	Traffic 30-minute (TRFC30) Report, Section 60	OVFL	This measurement is the number of times an attempt is made to use a tone transceiver with no idle tone transceiver available. This includes the requests that are removed from a queue without being satisfied.
	TRFC30 Report, Section 60	USG	This usage measurement (10-second scan) is the total amount of time that all tone transceivers per SM are in use.

NOTE:
Section 60 of the 5ESS Switch TRFC30 Report not only measures VPA, but also measures Incoming Calling Line Identification and Visual Message Waiting Indicators for analog lines. The report makes no attempt to separate these categories and hence the network administrator cannot single out only VPA measurements.

9.37 The LEC network administrator should periodically monitor the measurements shown in the table on the previous page to determine whether or not VPA testing is being denied due to lack of VPA circuits. Two areas are to be monitored: usage and overflow.

9.38 In monitoring VPA circuit usage, the LEC network administrator should establish a usage threshold (for example, 70 percent) per the office busy hour. If the usage measurement continually exceeds (taking into account peak periods) this threshold, more VPA circuits should be engineered and installed.

9.39 In monitoring VPA circuit overflow, these counts should typically be zero (indicating every VPA test engaged the services of a VPA circuit) taking into account unusual peak periods. If these counts are consistently nonzero, the LEC network administrator should establish an overflow threshold needed to maintain a given degree of service. If the overflow trend is continually exceeding this threshold, more VPA circuits should be engineered and installed.

10. Trunk Hunting

10.01 It is operationally important that hunting for an idle trunk be performed from opposite directions of the 2-way trunk facility to minimize the possibility of glare. To understand this, let us consider the example below where both switches perform a trunk hunt in the same direction.

The following conditions apply in the example:

(a) There are **500** trunk members between the two offices.

(b) Both offices start their hunt with trunk member **0** and forward hunt to the highest numerical trunk member until an idle trunk is found.

(c) There are **409** trunks currently busy with conversations in progress.

(d) Both offices attempt to originate a call at approximately the same instant.

10.02 If both offices attempted to seize trunk member **410** simultaneously, glare will occur. Appropriate glare control would resolve the problem allowing one office to seize trunk member **410** while the other office hunts for the next idle trunk member (that is, **411**). Every time calls originate from both offices simultaneously, this scenario is replayed.

10.03 The same situation holds true if both offices perform reverse trunk hunting from the highest numerical trunk member to the trunk member **0**.

10.04 To correct this situation, change Office **A** to forward hunting from trunk member **0** and Office **B** reverse hunting from the highest numerical trunk member. The probability of glare is greatly reduced. Only when all trunk members but one are busy is glare possible. Trunk hunting on 2-way trunks should always be performed in the opposite directions by the opposing ends of the trunk.

10.05 Table 3-AA summarizes the necessary recent changes for populating trunk hunting data.

Table 3-AB. Hunting Data Recent Changes

Office Type	Function/ View	Keyword/ Field	Description
1A ESS™ Switch	RC:TG	REVH	If "Y" the hunt for an idle trunk starts at the highest numerical trunk member. Likewise, if "N" the hunt should start at trunk member 0.
4ESS™ Switch	RC:TSG	REV	If "Y" the hunt for an idle trunk starts with the highest numerical trunk member. Likewise, if "N" the hunt should be started at trunk member 0.
5ESS® Switch	5.1	HUNTTYPE	Valid hunt types for 2-way SS7 trunks include: 2WF—forward hunting for trunk group <= 96 members 2WB—reverse hunting for trunk group <= 96 members LGFD—forward hunting for trunk groups > 96 members LGBD—reverse hunting for trunk groups > 96 members

Special Considerations

10.06 The *4ESS Switch TG-4 Translation Guide* recommends that trunk hunt for 2-way trunk subgroups be based on the alphabetic value of the CLLI code. By this recommendation, the switch with the lower (alphabetical) CLLI code hunts in the reverse direction (**REV = "Y"**). Regardless of the convention, it is important to always hunt in opposite directions on each end of the trunk group.

10.07 In an SS7 network, trunk hunt and glare settings are independent. That is, the hunt direction does not affect glare resolution. As mentioned above, all switches provide the flexibility of specifying hunt direction.

11. Circuit Query

11.01 A circuit query, sometimes referred to as trunk query, verifies the consistency of the call processing trunk states and trunk maintenance states at both ends of an SS7 trunk. State consistency, however, does not imply that the states at both ends are identical. Circuit query checks the states at both ends of a trunk and determines if an acceptable state combination exists. If an unacceptable combination exists, the switch initiating the circuit query takes the necessary corrective action to put both ends into one of the valid state combinations.

11.02 For the 1A ESS switch and 4ESS switch, circuit query settings are made on a per office basis. The 5ESS switch allows circuit query settings to be made on a trunk group basis. Table 3-AB summarizes the necessary recent changes for populating circuit query data.

Table 3-AC. Circuit Query Data Recent Changes

Office Type	Message/ View	Keyword/ Field	Description
1A ESS™ Switch	RC:POINTC	CQA	The field indicates whether or not the SS7 trunk query test is allowed on a per-office (that is, Point Code) basis. Circuit query is performed on one trunk at a time.
4ESS™ Switch	-	-	Audits 95 and 96 routinely query the whole office. Inhibiting the audits stops the queries from running.
5ESS® Switch	5.1	TRK QUERY	This field indicates whether or not the SS7 trunk query interoffice audit should run on this trunk group. If the audit is allowed to run on a trunk group, this field should be set to "Y"; otherwise, it should be set to "N". Circuit query is performed on 24 trunks at a time.
	8.15	TRK QRY AU	This field specifies the time interval between queries and ranges from 20 to 20,000 seconds.

11.03 Requirements for circuit query are specified in Bellcore's TR-NWT-000317, *Switching Systems Requirements for Call Control Using the Integrated Services Digital Network User Part.*

11.04 Circuit query in the 1A ESS switch is performed once per day between the hours of 8:00 p.m. and 6:00 a.m. To inhibit the query for a particular connecting office is as simple as specifying "no" in the CQA field of recent change message **RC:POINTC**.

NOTE:
The 1A ESS switch provides the following manual options:

- TNN—Trunk Network Number
- DPC—Destination Point Code
- TG—Trunk Group.

11.05 Circuit query in the 4ESS switch is routinely performed several times per day as a function of office size, the number of trunks, and the available real time (Audit 95). In addition, one trunk in each subgroup is queried also as a function of office size, the number of trunks, and the available real time (Audit 96). To inhibit the queries, refer to the **INH:AUD** and **OP:AUDSTAT** messages in the IM-4A000-01, *4ESS Switch Input Message Manual,* and the OM-4A000-01, *4ESS Switch Output Message Manual,* respectively. Likewise, to allow the inhibited audits to execute, refer to the **ALW:AUD** and **OP:AUDSTAT** messages in the same documents as above, respectively.

NOTE:
The 4ESS switch Audit 96 can be manually executed with the **AUD:NUM** input message. The 4ESS switch Audit 95 cannot be manually demanded.

11.06 Circuit query in the 5ESS switch is also routinely performed based on the "**TRK QRY AU**" value in recent change view 8.15. The circuit query progresses through allowed trunk groups (that is, **TRK QUERY** = "**Y**") 16 trunk members at a time.

NOTE:
A manual circuit query request can progress through 1-32 trunk members at a time.

11.07 To inhibit circuit query in a 5ESS switch for a particular trunk group, set the "**TRK QUERY**" value to "**N**" on recent change view 5.1.

11.08 As a general guideline, circuit query should be allowed on all trunks throughout the office unless severe service degradation is apparent.

Trunk Translation Test

11.09 The trunk translation test, commonly known as the Circuit Validation Test (CVT), is a manual request used to ensure that connecting switches have consistent translation data in order to place a call over a specified circuit. The test does not use the actual physical trunk path during the test, but instead transmits the translation data between connecting switches through the SS7 signaling links. For additional information on performing the test, refer to Chapter 6, "Circuit Validation Test".

11.10 Unless otherwise specified, inserting a new 5ESS switch trunk group using recent change view 5.1 defaults the **TRANS TEST** field to "**N**". This inhibits the craft from manually requesting the test over all members of the associated SS7 trunk group. The end result is that unless this field is set to "**Y**", execution of the translation test on any member of the trunk group is inhibited.

11.11 As a general guideline the trunk translation test should be allowed on all SS7 trunks throughout the office. This enables maintenance craft to validate translation data between office for a new trunk or for a trunk experiencing problems.

NOTE:
The 1A ESS switch and 4ESS switch do not have this test blocking option. Maintenance craft may request the test at any time over any trunk group member (1A ESS switch) or trunk subgroup member (4ESS switch).

12. Tone and Announcement Treatment

12.01 If during call setup [before sending Address Complete Message (ACM)] the connection cannot be completed or maintained, a "tone/announcement (T/A) treatment" is initiated. One form of this treatment is the return of an SS7 Release (REL) message with a cause indicator explaining why the call could not be completed. Another form of treatment is an inband T/A.

12.02 The following sections describe REL messages versus T/A handling in Lucent Technologies switching products.

1A ESS Switch

12.03 Whether an inband T/A is provided or a REL message is sent for failures detected in the 1A ESS switch itself will depend on a combination of Office Options and/or an IAM interworking indicator.

NOTE:
In the situation where the 1A ESS switch is providing a tandem connection, any REL message received from the terminating direction will be passed on through to the originating direction.

A. 1A ESS Switch Treatment

12.04 The following list summarizes generic software release 1AE11 and later software handling of all incoming SS7 calls that fail to complete in the 1A ESS switch:

(a) If the call encounters a "busy" condition and the incoming IAM indicates "no interworking encountered" (No. 7 signaling all the way), a REL message with a cause value of **17** indicating "user busy" is sent.

(b) For **1AE11.05** and earlier, if the call encounters a "busy" condition and the incoming IAM indicates "interworking encountered", call processing looks at Office Option **LCLTNOT** to determine the appropriate release treatment.

— If **LCLTNOT** is set to **"0"**, a REL message with a cause value of **17** indicating "user busy" is sent.

— If **LCLTNOT** is set to **"1"**, the switch provides inband busy tone treatment.

— For **1AE11.06** generic and later, if the call encounters a "busy" condition and the incoming IAM indicates "interworking encountered", call processing looks at office option **"BUSYANNC"** to determine the appropriate release treatment. The options are:

— If **BUSYANNC** is set to **"0"**, a REL message with a cause value of **17** is sent, indicating **"user busy"**.

— If **BUSYANNC** is set to **"1"**, the switch provides inband busy tone treatment.

— For calls which route to the Route Indexes (shown in the Table 3-AC), a REL message with the indicated cause value is sent, provided one of the following conditions is true:

Condition 1: The incoming IAM indicated "ISDN User Part used all the way" and Office Option **LCLTALL** is set to **"0"**.

Condition 2: The incoming IAM indicated "ISDN User Part *not* used all the way" and Office Option **LCLTNOT** is set to **"0"**.

If neither condition is true, the switch provides the appropriate inband T/A treatment as shown in Table 3-AC.

Table 3-AD. 1A ESS Switch Treatment—Route Indexes

Route Index	"Name"	Cause Value
80	Overflow (reorder)	"Temporary failure"
81	Common overflow	"Temporary failure"
89	Vacant code	"No route to destination"
180	No circuit	"No circuit available"
183	Intertoll no circuit	"No circuit available"
185	Intertoll vacant code	"No route to destination"

— For Inter-LATA calls, if a terminating LATA subtending screening failure is encountered (that is, Pseudo-Route Index 108) and the incoming IAM was received from an Interexchange Carrier (IC) switch, call processing looks at the IAM interworking indicator and one of two trunk group indicators, **TLSALL** or **TLSNOT**, to determine the appropriate release treatment.

NOTE:
Subtending screening analyzes the called party address to determine if it is directly connected (in which case call completion is attempted) or served by a subtending end office (in which case the call is routed to that end office for completion).

- — If the incoming IAM indicated "no interworking encountered, Signaling System 7" and **TLSALL** is set to "**0**", a REL message with cause value of **34** indicating "no route to destination" is sent.
- — If the incoming IAM indicated "no interworking encountered, Signaling System 7" and **TLSALL** is set to "**1**", the switch will provide the appropriate inband T/A.
- — If the incoming IAM indicated "interworking encountered", and **TLSNOT** is set to "**0**", a REL message with cause value of **34** indicating "no route to destination" is sent.
- — If the incoming IAM indicated "interworking encountered", and **TLSNOT** is set to "**1**", the switch will provide the appropriate inband T/A.

— For any failure condition other than those mentioned above, an inband T/A is provided by the switch.

12.05 For more detail about the Office Options mentioned above, refer to TDA Form 1500D in the TG-1A, *Translation Guide, 1A **ESS** Switch.* For more information concerning **TLSALL** and **TSLNOT**, refer to 231-318-375, *SS7 Integrated Services User Part and Network Interconnect Implementation and Trunk Conversation.*

4ESS Switch

12.06 Whether an inband T/A is provided or a REL message is sent for failures detected in the 4ESS switch itself will depend on three factors: (1) whether the incoming IAM crossed a network boundary, (2) whether or not the incoming trunk is an SS7 trunk, and (3) whether an Address Complete Message (ACM) has been sent to the incoming switch.

⇒ NOTE:
Provided that the incoming trunk was an SS7 trunk, the 4ESS switch will pass through any REL message received from a subsequent (terminating) switch to the incoming switch. If the incoming trunk is not an SS7 trunk and a REL message has been received from the terminating connection indicating a failed call attempt, the 4ESS switch will provide inband T/A.

A. 4ESS Switch Access Tandem Call Failure Treatment

12.07 In the same offices as noted above, Inter-LATA treatment is offered by individual Trunk Subgroup (TSG).

12.08 The appropriate action (REL or T/A) is defined on an individual TSG basis in RC 100 Form or ODA Form 401A. Two fields have been added to the TSG, "Backward Failure Treatment ISUP All The Way" (BFTIS) and "Backward Failure Treatment Not ISUP All The Way" (BFTNI), to achieve a more versatile treatment of an individual TSG.

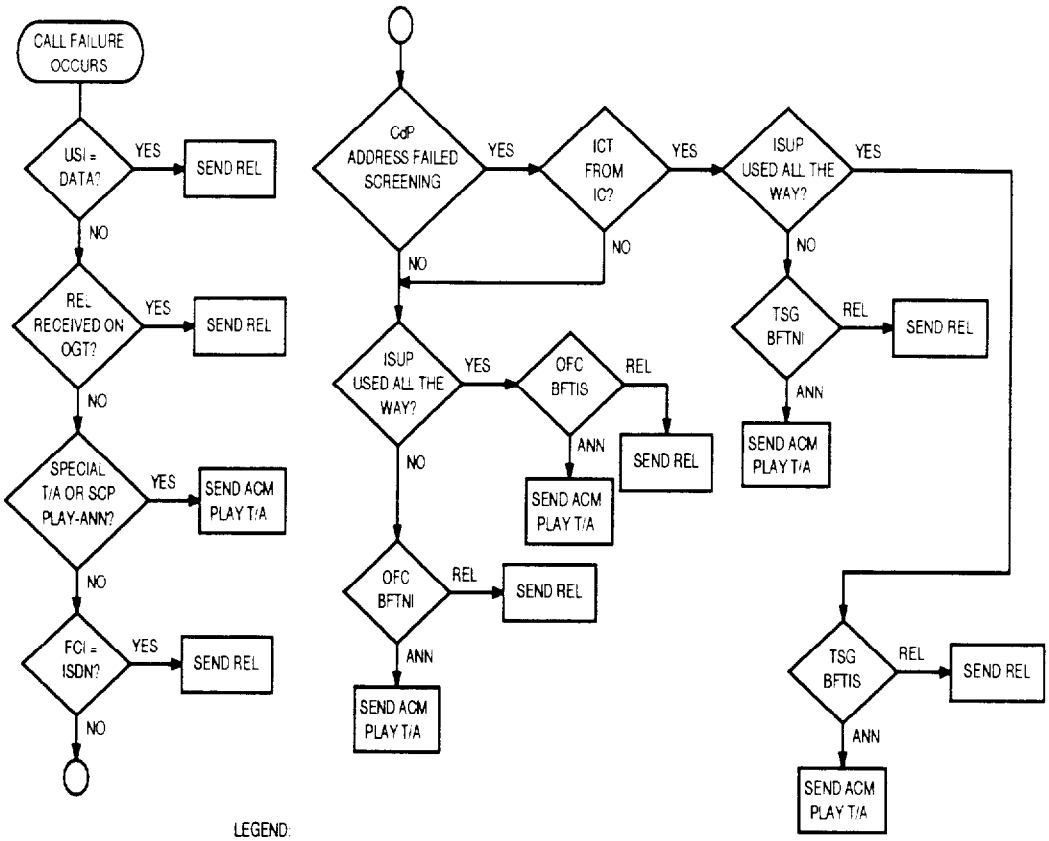
- BFTIS — This field specifies the action to be taken on a failed call when ISUP signaling is used for the entire call. This field is checked only when the Incoming Signaling Characteristic (ISC) is ISUP and the Type of Trunk (TOT) is Other Carrier Connecting (OCC). Valid entries in this field are:
  - — Blank or **REL** — Send release message with cause values.
  - — **ANN** — Play appropriate announcement.
- BFTNI — This field specifies the action to be taken on a failed call when ISUP signaling is **NOT** for the entire call. Use this field only when the incoming trunk ISC is ISUP and the TOT is OCC. Valid entries in this field are:
  - — Blank or **ANN** — Play announcement.
  - — **REL** — Send release message with cause value.

12.09 Figure 3.5 indicates the decisions that will take place depending on the conditions indicated. These conditions only apply when the incoming trunk is ISUP and the TOT is OCC.

12.10 In the present 4ESS switch generic software release, Intra-LATA SS7 calls are handled based on the ISUP indicator in the incoming IAM and the office parameter values of BFTIS and BFTNI.

12.11 BFTIS and BFTNI were added to office parameters (ODA Form 406Z) to allow for consistent Intra-LATA call failure treatment at the office level. Field descriptions for BFTIS and BFTNI are the same as those described for TSG fields. Field values cannot be changed using RC forms. The treatment at office level is not dependent on the TOT being OCC (refer to Figure 3-5).

⇒ NOTE:
The appearance of "CdP Address Failed Screening" and "ICT from IC" checks indicate the existence of Network Interconnect (NI) functionality.



LEGEND:

ACM	Address Complete Message
ANN	Announcement
BFTIS	Backward Failure Treatment ISUP All The Way
BFTNI	Backward Failure Treatment Not ISUP All The Way
CdP	Called Party Number
FCI	Forward Call Indicator
IC	Interexchange Carrier
ICT	Incoming Trunk
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
OFC	Office Option
OGT	Outgoing Trunk
REL	Release
SCP	Service Control Point
T/A	Tones and Announcements
USI	User Service Information

Figure 3-5. 4ESS Switch SS7 Call Failure Treatment at LEC Access Tandem (Incoming Trunk Is SS7)

5ESS Switch

12.12 The release treatment provided by a 5ESS switch will depend on the type of switch (AT, EO, and TOLL) and the type of call failure. For SS7 calls receiving *intercept* treatment, the 5ESS switch will return a backward ACM to allow the talking path to be established and provide the necessary T/A over talking path. The 5ESS switch provides inband tone T/A intercept treatment on a per Normalized Office Code (NOC) basis using TG-5 Form 5501 and Recent Change View 8.2 as shown in Table 3-AD.

Table 3-AE. Inband Tone/Announcement Treatment

TG-5 Form 5501	RC View 8.2	Description
REG ICPT RTI	REG ICPT RI	Regular Intercept (for example, Directory Number recently changed)
BLANK NBR RTI	BLANK NBR RI	Blank Number (for example, Directory Number not assigned)
OOS RTI	OOS RI	Out Of Service (for example, trouble)
DENY RTI	DENIED TERM	Deny Termination

Call Failure Tone/Announcement Indicator

12.13 When a call setup failure is encountered in an exchange, based on the type of failure and the type of exchange (Toll, Access Tandem, and End Office), one of five preset flag (indicator) values is used to determine if the exchange should play a T/A or return a REL message with the cause. Five of these indicators (Table 3-AE) are applicable to a Terminating End Office (TEO) or to an Access Tandem (AT).

Table 3-AF. Call Failure Tone/Announcement Indicator

Indicator	TG Form	RC View	Used In Office Type	Value Handling
NI ANNC	5202-2	5.1	TEO,TAT	N(d)—Send REL with cause. Y—Send inband T/A.
NI IW REL	5202-4	5.1	TEO,TAT	N(d)—Send inband T/A. Y—Send REL with cause.
LEC ANNC	5509	8.15	TEO, TAT OAT	N(d)—Send REL with cause. Y—Send inband T/A.
LEC IW REL	5509	8.15	TEO, TAT	N(d)—Send inband T/A. Y—Send REL with cause.
BUSY ANNC	5509	8.15	TEO	N(d)—Send REL with cause. Y—Send inband T/A.
(d) — Default Value OAT — Originating Access Tandem TAT — Terminating Access Tandem TEO — Terminating End Office				

Description of Indicators

NI ANNC

12.14 The "NI ANNC" Trunk Group indicator is used for Called Number screening occurring at TAT or TEO directly connected to the IEC. This indicator is checked if the call originated from a Non-ISDN user and is routed using "ISUP7 Signaling all the way" (no interworking). Tone/Announcement can be sent over the trunk; however, if the trunk is "ISDN-data", T/A may not be sent.

NI IW REL

12.15 The "NI IW REL" Trunk Group indicator is used for Call Number screening failures occurring at a TAT or TEO directly connected to an IEC. This indicator is checked if interworking (not ISUP signaling all the way) is encountered in the call route.

LEC ANNC

12.16 The "LEC ANNC" indicator is a global office parameter used for certain call failures at a TEO, TAT, or OAT. This indicator is checked if the call originates from a Non-ISDN user and is using all SS7 circuits (no interworking).

LEC IW REL

12.17 The "LEC IW REL" indicator is a global office parameter used for certain call failures at a TEO or TAT. This indicator is checked if interworking (not ISUP signaling all the way) is encountered in the call route.

BUSY ANNC

12.18 The "BUSY ANNC" indicator is a global office parameter used when a "user busy" connection is encountered at the TEO. This indicator is checked if interworking was encountered before reaching the TEO.

Summary of Tone/Announcement Treatment

12.19 The following paragraphs and tables summarize the final handling treatment options. Information contained in this section applies to Voice calls that are non-ISDN originated. In general, Data calls return **REL**ease and ISDN originated voice calls return **REL**ease unless a specialized announcement is required.

A. Intra-LATA Call Treatment

12.20 Call failure treatment for intra-LATA calls for Lucent Technologies switches is shown in the Table 3-AF. Each option allows a choice of sending an SS7 **REL**ease message or providing an announcement. The RC Form and field for each option are shown in brackets.

Table 3-AG. Call Failure Treatment for Intra-LATA Calls

Switch	Options	Form/Field or Remarks
1A ESS™	Offers Three Office Options	
	ISUP All the Way	[LCLTALL]
	ISUP Not All the Way	[LCLTNOT]
	Busy, Interworking	[BUSYANNC]
4ESS™	Offers Two Office Options	
	ISUP All the Way	[ODA Form 406Z—BFTIS]
	ISUP Not All the Way	[ODA Form 406Z—BFTNI]
5ESS®	Offers three Office Options	
	ISUP All the Way	[8.15 LEC ANNC]
	ISUP Not All the Way	[8.15 LEC IW REL]
	Busy, Interworking	[8.15 BUSY ANNC]

B. Inter-LATA Call Treatment

12.21 If the called party address fails the screening, the determination whether to provide a tone or announcement or to RELease the incoming circuit should be configurable to be set, based on incoming (from IXC) circuit group and the coding of the received ISDNUP indicator. Options shown in Table 3-AG apply to call failure treatment for inter-LATA calls in Lucent Technologies switches.

NOTE:
Called party address screening is also known as "terminating screening" or "subtending screening".

12.22 Each option allows a choice of sending an SS7 **REL**ease message or providing tone and announcement. The RC Form and field for each option are shown in brackets.

Table 3-AH. Call Failure Treatment for Inter-LATA Calls

Switch	Options	Form/Field or Remarks
1A ESS™	Offers two Trunk Group Options	
	ISUP All the Way	[RC:TG TLSALL]
	ISUP Not All the Way	[RC:TG TLSNOT]
4ESS™	Offers two Trunk Group Options	
	ISUP All the Way	[TSG-BFTIS]
	ISUP Not All the Way	[TSG-BFTNI]
5ESS®	Offers two Trunk Group Options	
	ISUP All the Way	[5.1 NI ANNC]
	ISUP Not All the Way	[5.1 NIIW REL]

12.23 Generic software release 5E6 option controls can be used to control classes of call failures. Generic software releases 5E7 and 1AE11 Trunk Group options only control called party address screening failures. Other call failures involving IXCs are not controlled by the TG option and are subject to the option described for intra-LATA calls.

13. Administration of the A and B Signaling Bits

13.01 The **A** and **B** bits are signaling bits contained in the T1 voice data stream. Per-Trunk Signaling (PTS) between switches over T1 trunks is accomplished by "robbing" the **A** and **B** bits from the voice data for signaling. In PTS, these bits indicate the on-hook and off-hook state of the trunks.

13.02 On Integrated T1 trunks using SS7 signaling, the **A** and **B** bits are not used by the switches for signaling information (Table 3-AH). However, certain transmission equipment, including the Dial Pulse Terminating channel unit in the D4 Channel bank, requires the **A** and **B** bits to change to the off-hook state to close the voice path. Thus, the bits are set as indicated in the following:

1A ESS switch — The **A** and **B** bits are always set to match the on-hook or off-hook states of SS7 calls using the trunk.

4ESS switch — The **A** and **B** bits are normally allowed to "float" unless connected to a Digroup terminal, then they are set to a steady "off-hook". When connected to a 1A ESS switch, they are set to steady "on-hook". When connected to an IXC, the TSG option is set to either steady "on-hook" or "float" (default).

5ESS switch — The administration of the **A** and **B** bits depends on the Idle state field of the trunk member translations in the office data base. This field is changed via the Recent Change View 5.5.

Table 3-AI. Recent Change View 5.5 for A and B Signaling Bits

Idle State = ON	Idle State = OFF
The A and B bits are both held in the on-hook state.	The A and B bits change to match the on-hook and off-hook states of SS7 calls that use the trunk.

14. Network Interconnect (Internetwork SS7 Signaling)

14.01 The Network Interconnect (NI) feature provides the capability for SS7 messages to be passed between SS7 signaling networks with different network identifiers. The 2ASTP generic release 2STPD5 provides the interconnection of SS7 networks with the full Gateway Screening capabilities defined in Bellcore's TR-TSY-000082.

The 1A ESS, 4ESS, and 5ESS switches use the internetwork extension of SS7 signaling to allow internetwork, inter-LATA SS7 ISUP trunk signaling to an IEC as defined in Bellcore's TR-NWT-000394. These switches also support intra-LATA SS7 ISUP trunk signaling as defined in Bellcore's TR-NWT-000317 between two networks, provided both networks are in the same LATA. Refer to Table 3-AI to determine the recent changes needed in switches for inter-LATA and intra-LATA internetwork trunks.

14.02 Interexchange Carriers and International Carriers are collectively known as IXCs.

14.03 An example of a LEC Interconnect configuration is shown in Figure 3-6. This example and associated data are used throughout this chapter. The network data is shown in the example **OP:C7NET** output in Chapter 6, "Displaying Routing Data".

14.04 For a detailed description of the SS7 Network Elements, refer to 256-002-100, *Switching Products Common Channel Signaling 7, Information Guide.*

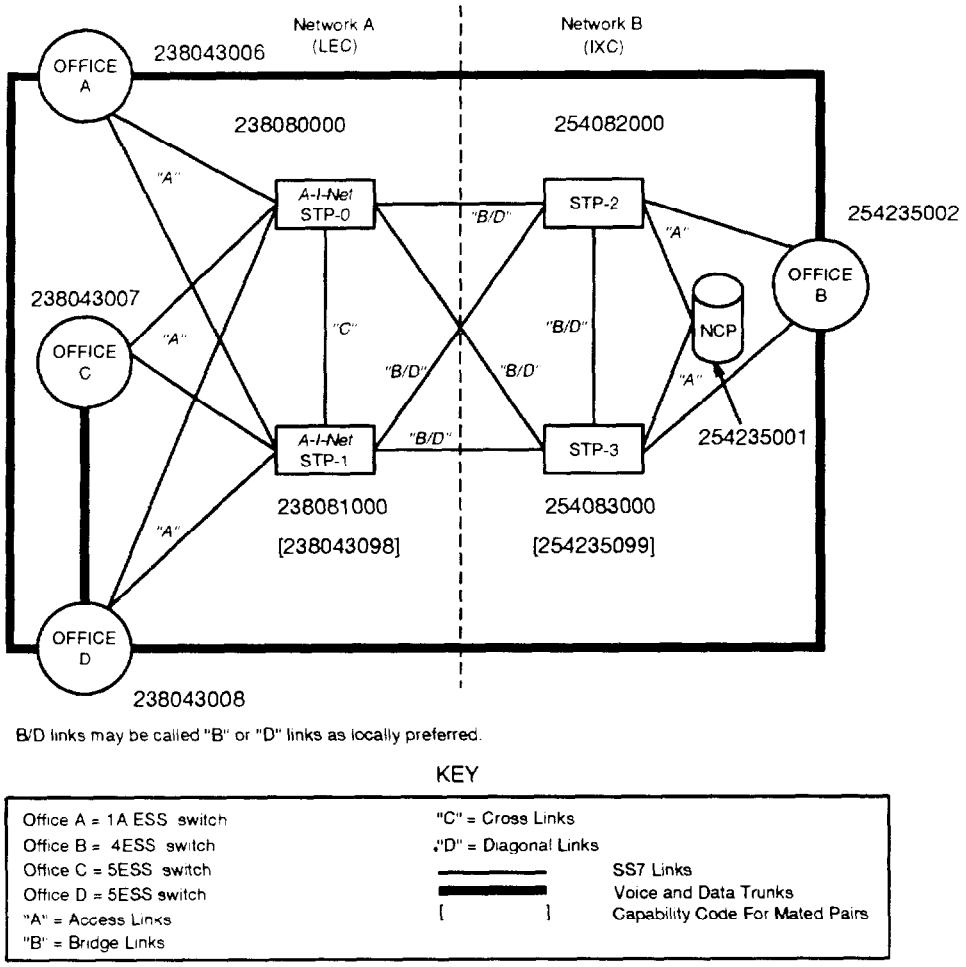


Figure 3-6. Sample LEC Network Interconnect Configuration

Table 3-AJ. RC Views/Functions for Consistent Internetwork SS7 Trunk Data

Data Field	Data Type	Trunk Type*	1A ESS™ Switch	4ESS™ Switch	5ESS® Switch
Calling Party Number	Switch	IXC	RC:ICCB	RCFORM 10x†	View 10.2
Billing Number	Switch	IXC	RC:ICCB	RCFORM 10x†	View 10.2
MAUUI (ATP/UUI)	Switch	IXC	RC:TG	N/A	View 5.1
Tone & Announcement	Switch	IXC	RC:TG	RCFORM 10x†	View 10.1
Circuit Code Parameter	Switch	IXC	RC:PSWD	RCFORM 301	View 10.2
Circuit Code to 0ZZ/1NX (Access Tandem)	Switch	IXC	RC:PSWD	RCFORM 524‡	View 10.23
0ZZ/1NX to Circuit Code	Switch	1XC	RC:PSWD	RCFORM 335‡	View 10.2
ISUP Timers	Switch	IXC	RC:PSWD	RCFORM 800	View 8.15

* IXC = Inter-LATA, Internetwork SS7 trunk (TR-394) to IC or INC. INTRA = Intra-LATA, Internetwork SS7 trunk (TR-317) between LECs

† The 100 series RC form number depends on whether the function is ADD or CHG, and trunk direction.

‡ For MF to SS7 interworking only.

14.05 Because ISUP signaling can deliver the calling party number to the terminating switch, the LASS features **ICLID**, **BCLID**, and **COT** can be extended across network and LATA boundaries.

14.06 There are currently no requirements defined to address inter-LATA Transaction Capabilities Application Part (TCAP) or SCCP signaling. The **LASS AR/AC** and **LASS SLE** features use TCAP signaling and, therefore, have not yet been defined for inter-LATA use.

Internetwork, Inter-LATA ISUP Trunks

14.07 The ISDN trunk signaling protocol was initially implemented to carry only those calls made within a single LEC, as defined in Bellcore's TR-NWT-000317. Thus, inter-LATA and international calls must use Equal Access Multifrequency (EAMF) Signaling Protocol defined in Bellcore's TR-NWT-000690 FSD20-24-000 and implemented as the Carrier Interconnect feature in the 1A ESS, 4ESS, and 5ESS switches. Inter-LATA calls over ISUP trunks are possible in 1A ESS, 4ESS, and 5ESS switches beginning in generic software releases 1AE11, 4E14, and 5E6 respectively. This feature, known as Network Interconnect, allows LECs to interface with IXCs using SS7 signaling.

Internetwork, Intra-LATA ISUP Trunks

14.08 The Network Interconnect feature also provides the ability to signal SS7 across network boundaries for Intra-LATA ISUP Calls. The ISUP protocol used for these calls is defined in Bellcore's TR-NWT-000317.

Signaling Network Interconnection

14.09 When implementing SS7 trunks between switches in different networks, the signaling networks must first be interconnected. This is accomplished by **D-links** between the LEC's gateway STPs and the IXC's gateway STPs. To interconnect two LEC networks (LEC **A** and LEC **B**) for intra-LATA SS7 trunks, **D-links** are used between LEC **A's** gateway STPs and LEC **B's** gateway STPs. Gateway STPs provide the ability to selectively screen incoming internetwork SS7 messages.

Network ID Data for Internetwork SS7 Trunks (IXC and Intra-LATA)

14.10 After the LEC switch has been connected to the other signaling network through the gateway STPs, the network ID of the far-end SS7 network must be identified in the LEC switch's CNI data base. The first three digits of Point Code are the Network ID, which is assigned by Bellcore to uniquely identify each SS7 network. For the purposes of this document, the Network ID of the LEC switch whose data base is being populated is referred to as the local Network ID. All other Network IDs are referred to as nonlocal Network IDs.

14.11 A nonlocal Network ID must be assigned to the CNI data base for each nonlocal network to which the LEC has SS7 trunks. When populating the nonlocal Network IDs in the CNI data base, refer to Table 3-AI for the recent change view/functions.

Point Code Data for Internetwork SS7 Trunks (IXC and Intra-LATA)

14.12 Point Code data for ISUP trunks to a switch in another network is populated the same as for intranetwork trunks except that the Network ID portion of the far-end Point Code is nonlocal. For the requirements for populating Point Code data, refer to paragraph 3.08.

Trunk Circuit Identification Code (TCIC) Data for Internetwork SS7 Trunks (IXC and Intra-LATA)

14.13 A TCIC is a numeric value assigned to each SS7 internetwork SS7 trunk. The TCIC assignment must be identical in both the LEC office (from the local network) and the distant office (from the nonlocal network) connected to a given trunk circuit. For the requirements for populating circuit identification data, refer to Part 8.

CLLI Code Data for Internetwork SS7 Trunks (IXC and Intra-LATA)

14.14 *Common Language* CLLI code data for internetwork SS7 trunks is populated in the same manner as CLLI code data for intranetwork trunks, except that any far-end CLLI code data represents locations in a nonlocal SS7 network. For the requirements for populating CLLI code data, refer to Part 4.

Voice Path Assurance Data for Internetwork SS7 Trunks (IXC and Intra-LATA)

14.15 Voice Path Assurance (VPA) data elements for internetwork SS7 trunks must be consistent in both the LEC office (from the local network) and the distant office (from the nonlocal network) to ensure they agree on the type of test being run. For the requirements for populating VPA data, refer to paragraph 9.13.

Glare Data and Hunt Direction for Internetwork SS7 Trunks (IXC and Intra-LATA)

14.16 The Glare and Hunt Direction data elements for internetwork SS7 trunks must be coordinated between the LEC office (from the local network) and the distant office (from the nonlocal network) that are connected to a given trunk circuit. In the event that a glare condition occurs, both switches must know which has control over the transmission path. For the requirements for populating Glare and Hunt Direction data, refer to paragraph 9.08.

Link and Linkset Data needed for Internetwork SS7 Trunks

14.17 Link and linkset data for SS7 SLKs in the LEC switches is populated in the same manner as link and linkset data for intranetwork links for signaling network interconnection. For the requirements for populating link and linkset data, refer to Part 5.

Cluster Data for Internetwork SS7 Trunks (IXC and Intra-LATA)

14.18 Cluster data for internetwork SS7 trunks must be defined in the same manner as cluster data for intranetwork trunks, except that the network identification used to assign cluster data in the CNI data base is nonlocal. For the requirements for populating cluster data, refer to Part 6.

Billing Number Data for Internetwork SS7 Trunks (IXC Only)

14.19 A LEC switch can optionally send the charge number, using Automatic Number Identification (ANI) in EAMF, to a Carrier. Lucent Technologies switching products offer the ability to optionally send the Billing number parameter in the IAM if the carrier has subscribed to receive the charge number. Refer to Table 3-AI for the requirements

⚠ CAUTION:
For the data items described in this paragraph and the next two paragraphs each switch type has an option to control the contents of SS7 messages. The setting of these fields, at switches serving as tandems must be coordinated with the end office switches. It is possible to allow some data on an end office message and have the tandem remove it as it sends it to the carrier.

Calling Party Number Data for Internetwork SS7 Trunks (IXC Only)

14.20 A LEC switch can optionally send the Directory Number (DN) of the Calling Party Number (CPN) to a Carrier. Lucent Technologies switches offer the ability to screen out the Calling Party Number parameter from the IAM if the carrier has not subscribed to receive CPN. Refer to Table 3-AI for the requirements for populating the CPN screening option on SS7 messages to an IXC.

⚠ CAUTION:
The 1A ESS switch has an office option that overrides the capability for sending CPN intra-LATA as well as inter-LATA and is only set because of regulatory issues.

Message Associated User-to-User Information Data for Internetwork SS7 Trunks (IXC Only)

14.21 The 5ESS and 1A ESS switches acting as either end-offices or access tandems, and the 4ESS switch acting as an access tandem, have the ability to optionally pass Message Associated User-to-User Information (MAUUI) to an IXC . The MAUUI results when Q.931 Information Elements from an Integrated Service Digital Network (ISDN) Basic Rate Interface (BRI) or Primary Rate Interface (PRI) are mapped into the SS7 protocol for transport between ISDN equipped products. These Q.931 Information Elements are mapped into two SS7 parameters: User-to-User Information (UUI) parameter and Access Transport Parameter (ATP).

14.22 The UUI and ATP parameters are transparently carried through the SS7 network as optional parameters on the IAM, ACM, ANM, and REL messages. The UUI and ATP parameters have no effect on ISUP call processing and are only examined by the ISDN equipment on the receiving end.

14.23 The 1A ESS (AT) and 5ESS switches can optionally screen out MAUUI (UUI and ATPs) on a per-trunk group basis if the Carrier has not subscribed to receive MAUUI. Refer to Table 3-AI.

Tone and Announcement Treatment Data for Internetwork SS7 Trunks (IXC)

14.24 Calls from IXC switches that fail subtending screening (calls not allowed into the LEC network at this point) can optionally be returned to the carrier via a REL message, or the terminating switch can play a tone or announcement. Each switch provides a recent change capability to specify what action to take in this situation. For tone and announcement treatment data, refer to Table 3-AI and Part 12.

Circuit Code Data at End Offices for Internetwork SS7 Trunks (IXC Only)

14.25 An end office sends a Circuit Code value to an Access Tandem (AT) by signaling indirectly via an AT to an Interexchange Carrier/Incoming (IC/INC). The Circuit Code is a 4-bit field in the Transit Network Selector parameter of the IAM message. Circuit Codes are used by the AT, along with the TCIC, to determine the selected route to the Carrier. The Circuit Code is the inband Equal Access equivalent of **0ZZ** for domestic calls, and **1N'X** for international calls. When populating Lucent Technologies end-office LEC switch data bases to send a Circuit Code to the AT, refer to Table 3-AI for recent change messages.

Circuit Code to 0ZZ/1N'X Data at Access Tandem for Internetwork SS7 Trunks (IXC Only)

14.26 An Access Tandem (1A ESS and 5ESS switches only) receiving an incoming IXC SS7 trunk call from an end office must be able to translate the 4-bit Circuit Code into digits, for domestic or international calls. The Circuit Code is a field contained in the transit network selector parameter of the IAM message. The digits associated with a Circuit Code are used by the AT in conjunction with the trunk class of service codes to determine the selected route to the Carrier. When populating AT LEC switch data bases for the Circuit Code translations, refer to Table 3-AI for recent change messages.

ISUP Timers Data for Internetwork SS7 Trunks (IXC Only)

14.27 A changeable timer is provided for the release of the EXIT message to the originating switch. Refer to Table 3-AI. For the 4ESS switch, it is not necessary to put in an RC unless the default is not wanted (1000 msec or 1 second). This is true for 1A ESS switch also. The 5ESS switch default value is 300 msec or 0.3 second.

End Office Data for Internetwork SS7 Trunks (IXC Only)

14.28 Presently, trunks for Multifrequency Equal Access calls routed indirectly to an IC/INC may have the overlap outpulsing capability turned on. If these trunks are converted to SS7 signaling, the overlap capability must be turned off. For 5ESS switches, use view 10.2. For 1A ESS switches, use **RC:ICCB;CHG** message, **RTOVP NO**. Failure to do so could cause a nonfatal DB error message on the 1A ESS switch.

A-I-Net Products STP Full Gateway Screening Requirements

14.29 Beginning with the *A-I-Net* products STP Release 0, the STP provides the complete screening required for Network Interconnect Phase 1, in a capability known as Full Gateway Screening. The Enhanced Gateway Screening capability has been replaced with 12 new data base management system functions listed in Table 3-AJ.

Table 3-AK. Full Gateway Screening Data Base Management System Functions

Function	Description
affdst	Identifies the allowed affected PCs for Message Transfer Part (MTP) network management messages received on the incoming linkset.
afpcsn	Identifies the allowed PC/Subsystem Number (SSN) combinations for Signaling Connection Control Part (SCCP) management messages received on the incoming linkset.
alcdpa	Identifies all the allowed PC and SSN combinations for messages on which a global title translation was performed or which are routed on the SSN.
alcgpa	Identifies all the calling party address Point Code and SSN combinations which are allowed to transmit SCP messages on the incoming linkset.
alwdpc	Identifies all the PCs which are allowed to receive messages on the incoming linkset.
alwgtt	Identifies all the translation types for messages requiring GTT.
alwopc	Identifies all the PCs which are allowed to originate messages on the incoming linkset.
alwsio	Identifies combinations of the codes from the service information octet which are allowed on the incoming linkset.
blkdpc	Identifies the PCs which are not allowed to receive messages on the incoming linkset.
blkopc	Identifies the PCs which are not allowed to originate messages on the incoming linkset.
desdst	Identifies clusters and Point Codes in the local network that are designated destinations for nonlocal network management messages.
gtwyls	Identifies all linksets which may transport messages from another network, as well as linksets within the local network, on which screening is to be performed.

14.30 The function *gtwyls* is initially used to identify the linkset(s) terminating at the STP on which **incoming** message screening is to be performed. Specific screening data populated with the remaining eleven new functions depends on the extent of the interconnection agreements between the networks.

NOTE:
Gateway Screening is supported on SS7 Integrated Ring Node type link nodes only. For specific engineering information, refer to 270-750-202, *A-I-Net products STP Engineering Guide (Release 2).*

14.31 For specific data population dependencies and restrictions, refer to Chapter 5 of the 270-750-406, *A-I-Net* products *STP Data Base Administration Manual (Release 2).*

15. Small Network Specific Requirements

15.01 According to Bellcore TR-NWT-000246, an SS7 network that initially provides signaling for more than 75 signaling points (belonging to the network), or over the first 5 years provides signaling for 150 signaling points, is assigned a large network code. An SS7 network not meeting these requirements is assigned a small network code. To this end, NID codes 1 through 4 have been reserved for small network code assignments. The combination of the NID field and network cluster field uniquely identifies a particular small network. Small networks are assigned Point Codes starting with NID field code 1 and network cluster (CLU) field code 1, and incrementing.

15.02 Two scenarios have been identified for routing signaling messages to and from a small network and are described on the following pages. Routing data tables (Tables 3-AK and 3-AL) follow each scenario to which they apply. Switch routing networks (Figures 3-7 and 3-8) precede each routing data table to which they apply.

15.03 The two scenarios involve routing to/from a small network that has a different NID code than the switch (Nonlocal NID), and routing to/from a small network that has the same NID code as the switch (local NID).

15.04 For small network connection to large networks, follow the large network examples in the previous section. The same rules apply.

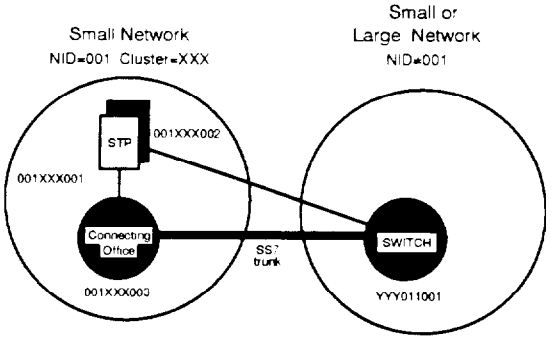


Figure 3-7. Switch Routing Values for Nonlocal Scenario

Table 3-AL. Routing Data For Nonlocal Network ID (NID)

Switch	AP/Switch Generic	Routing for Cluster XXX		
		View/Function	Field	Value
1A ESS™ Switch	1AP3F and later	ROUTE	MEMBER	Member # of STP1
			ROUTING FLAG	SMEMBER
			PRIMARY ROUTE	Linkset of STP1
		ROUTE	MEMBER	Member # of STP2
			ROUTING FLAG	SMEMBER
			PRIMARY ROUTE	Linkset of STP2
		ROUTE	MEMBER	Member # of Connected Office
			ROUTING FLAG	SMEMBER
			PRIMARY ROUTE	Combined Linkset #
4ESS™ Switch	4AP12 and later	MEMRTE	MEMBER ID	Member # from the Cluster
			PRIMARY ROUTE	Combined Linkset to the A-Link/ E-Link STP Pair
			ALT 1 ROUTE	Combined Linkset to the E-Link/ A-Link STP Pair
			ALT 2 ROUTE	Always Zero to indicate no ALT 2 Routing
5ESS® Switch	5E9 and later	15.18	MEMBER	Member # of STP1
			PRIMARY ROUTE	Linkset of STP1
		15.18	MEMBER	Member # of STP2
			PRIMARY ROUTE	Linkset of STP2
		15.18	MEMBER	Member # of Connected Office
			PRIMARY ROUTE	Combined Linkset #

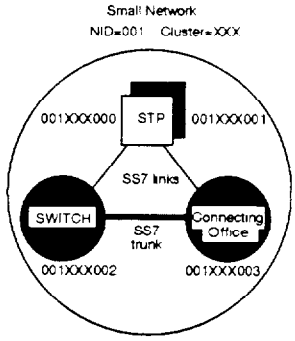


Figure 3-8. Switch Routing Values for Local Scenario

Table 3-AM. Routing Data For Local Network ID (NID)

Switch	AP/Switch Generic	Routing for Cluster XXX		
		View/Function	Field	Value
1A ESS™ Switch	1AP3F and later	ROUTE	MEMBER	Member # of STP1
			ROUTING FLAG	SMEMBER
			PRIMARY ROUTE	Linkset of STP1
		ROUTE	MEMBER	Member # of STP2
			ROUTING FLAG	SMEMBER
			PRIMARY ROUTE	Linkset of STP2
		ROUTE	MEMBER	Member # of Connected Office
			ROUTING FLAG	SMEMBER
			PRIMARY ROUTE	Combined Linkset #
4ESS™ Switch	4AP12 and later	MEMRTE	MEMBER ID	Member # from the Cluster
			PRIMARY ROUTE	Combined Linkset to the A-Link/ E-Link STP Pair
			ALT 1 ROUTE	Combined Linkset to the E-Link/ A-Link STP Pair
			ALT 2 ROUTE	Always Zero to indicate no ALT 2 Routing
5ESS® Switch	5E9 and later	15.18	MEMBER	Member # of STP1
			PRIMARY ROUTE	Linkset of STP1
		15.18	MEMBER	Member # of STP2
			PRIMARY ROUTE	Linkset of STP2
		15.18	MEMBER	Member # of Connected Office
			PRIMARY ROUTE	Combined Linkset #

16. Data Consistency Requirements for Connectionless Service

16.01 In addition to Integrated Services Digital Network—User Part (ISUP), SS7 services include a variety of capabilities that use the Signaling Connection Control Part (SCCP) protocol. An example of which is the Transaction Capabilities Application Part (TCAP) features.

16.02 The SCCP provides the ability to transfer user information between network signaling points that are not interconnected by physical circuits (for example, voice or data trunks). The origination of an SCCP message is identified by the calling party address. Likewise, the destination is identified by the called party address. Either address may contain a combination of Global Title (GT), Point Code, and/or Subsystem Number.

If the SCCP message is routed based on GT (for example, Translation Type plus digits), it is routed to the STP selected to translate the GT to an appropriate Destination Point Code (DPC) and Subsystem Number (SSN).

16.03 Performing a GTT at the STP eliminates the need for each switch to know the PC serving every Directory Number (DN) and SCP data base application in the network. After translation, the DPC provides the address of the next translation point (in the case of successive GTTs) or the address of the final destination along with SSN (in the case of a final GTT), to which the message is routed.

16.04 A summary of the required Recent Change views/functions is in Table 3-AM.

Table 3-AN. RC Views/Functions for Consistent Connectionless Service Feature Data

Consistency Item	1A ESS™ Switch	4ESS™ Switch	5ESS® Switch	*A-I-Net*® STP All Gen.	*A-I-Net* SCP
Point Codes of GTT STPs	GBLTT	GTTRAN	View 15.11	SELFID	SCP Submenu Select 4
Translation Types	GBLTT	RC:TOS	View 15.11 View 8.17	ORDGTT	na
Subsystem Numbers	SETSSN	RC:TOS	View 15.10 View 8.17	ORDGTT	SPMAN Submenu Select 2 or 3 SCP Submenu Select 8, 11
Cluster Data Additions	ROUTE	CLSROUT* ROUTE	View 15.9	ORDRTE Select 8	SCP Submenu O,A,& M Submenu

* Used for clusters only.

General Data Requirements

A. Selection of STPs to Perform Global Title Translations

16.05 By default, the local STP pair performs GTT for Lucent Technologies switches. It is possible, though, to implement GT routing in four ways:

(1) All GTTs are performed by the local STP pair (that is, the pair to which the switch is connected via **A-links**). Refer to Figure 3-1.

(2) All GTTs are performed by a remote STP pair (that is, a pair other than the local STPs).

(3) The GTTs are performed by an STP pair selected on a feature basis. For example, GTTs required for LASS could be performed by the local STPs, while GTTs required for Service Switching Point (SSP) 800 Service could be performed by the regional STPs.

(4) Intermediate GTTs and Gateway Screening.

16.06 For 1A ESS switching system details, refer to 231-361-026, *Common Channel Signaling 7, CNI Ring Implementation Guide.* For 5ESS switching system details, refer to 235-190-120, *5ESS Switch, Common Channel Signaling Services Features.* For 4ESS switching system details, refer to Lucent Technologies *4ESS Switch Translations Guide (TG).*

16.07 When populating GTT data, refer to Table 3-AM for a summary of recent changes.

16.08 In selecting the GTT STPs, Capability Codes (Alias Point Codes) can be used. Here, each of the STPs performing the GTTs is identified by the same (alias) Point Code, and signaling messages requiring GTT are sent to the STPs using the Capability Code identification. The use of the Capability Codes provides two distinct advantages.

16.09 First, if traffic is prohibited to one of the GTT STPs because all **A-links** to that STP are out-of-service, all the GTTs are handled by the other STP. When Capability Codes are not used, GTT traffic is normally shared between the STPs. If the links to one STP are down, the traffic destined for that STP is routed via the mate STP and the **C-links**. This results in additional signaling delay.

16.10 Secondly, if one of the STPs fails, fewer GTT messages are lost if Capability Code routing is used. Messages in-transit are routed to the mate.

16.11 An example of Capability Code routing can be found in 235-190-120, *5ESS Switch, Common Channel Signaling Services Features.*

16.12 It is important to note that when Capability Codes are used, the capability code value for the GTT STP must be specified as described earlier for the remote STP PCs. Likewise, at an *A-I-Net* products STP, the Alias List in the SELFID function must contain the respective Capability Code value as well. For procedural details, refer to 270-750-406 (*A-I-Net* STP), Release 2.

16.13 It is also important to note that if intermediate GTTs are performed in the *A-I-Net* products STP, a Subsystem Number of zero must be used in the STP that is performing the intermediate GTTs. The STP that performs the final GTT will overwrite the Subsystem Number with the appropriate data. The Subsystem value of zero is required in the intermediate STP to avoid false Subsystem test messages.

B. Translation Types

16.14 The Translation Type is a translator index used by the STP to derive DPC and SSN information from a GT message sent from a switch. Each TCAP feature (for example, LASS or SSP/800) is assigned a Translation Type by the Local Exchange Carrier Network Administrator. For a given TCAP feature, the Translation Type must be consistent between the switch and the STP. The full range of Translation Type values is 0 to 255 (STP is 0-254).

16.15 When populating Translation Type data, refer to Table 3-AM for a summary of recent changes.

C. Subsystem Numbers

16.16 The Subsystem Number (SSN) is the 3-digit value used to identify the specific application/feature at the switch or SCP that is sending or receiving an SCCP message. Subsystem information is included in both the calling and called party address portions of the SCCP message. The SSNs are assigned in each network and must take on values within a range prescribed by each Lucent Technologies product. A summary of these ranges is provided in Table 3-AN.

Table 3-AO. Valid SSN Ranges For Signaling Point Types

1A ESS™ Switch	4ESS™ Switch	5ESS® Switch	*A-I-Net*® STP
0-7, 232-254	0-7, 232-254	0-7, 232-254	0-7, 232-254

16.17 The SSN data is populated in the CNI data bases and in switch specific data structures. The SSN information stored in the CNI data base must be consistent with the SSN information stored in the Lucent Technologies switch or *A-I-Net* products STP data base. The SSN data must also be consistent between switches, STPs, and SCPs.

16.18 It is advisable that SSNs assigned to a specific application be consistent throughout the network.

16.19 When populating subsystem data, refer to Table 3-AM for a summary of recent changes.

D. Additions to Cluster Data

16.20 Assuming that cluster data is populated for ISUP functionality, additional cluster information must exist for the other destinations of SCCP messages (that is, LASS or SSP/800 messages). For ISUP requirements, refer to Part 6. Unique cluster values must be populated for the following:

(1) Clusters of the GTT STPs, if the GTTs are performed by a remote STP pair, or the clusters of any Capability Codes, if Capability Codes are being used.

(2) Cluster of the SCP data base, if applicable.

(3) Clusters of any SCCP message destinations within the network, if not previously populated. Cluster tables are populated only once for each unique cluster value.

16.21 When populating this cluster data, refer to Table 3-AM for a summary of recent changes.

17. LASS Specific Requirements

17.01 The LASS is a set of features providing special call handling. These features use the identity of the calling party to determine the appropriate handling for each call. Calling party information is in the Initial Address Message (IAM) signaling message associated with each call. Thus, ISUP is used as the basis for LASS interoffice services.

17.02 The LASS features include:

- Automatic Recall (AR)
- Automatic Callback (AC)
- Customer Originated Trace (COT)
- Calling Name Delivery (CNAM)
- Individual Calling Line Identification (ICLID)
- Bulk Calling Line Identification (BCLID)
- End-to-End Call Trace (EECT)

- Selective Call Forwarding (SCF)
- Calling Party Number Presentation Capability (CPNPC)
- Selective Call Rejection (SCR)
- Distinctive Alerting (DA)
- Selective Call Acceptance (SCA)
- Computer Access Restriction (CAR)
- Unidentified Caller Rejection (UCR).

NOTE:
The CPNPC capability is a special optional feature (non-LASS) that provides additional options to the "Privacy" feature.

17.03 General descriptions of each of the LASS features can be found in the appropriate *TR* and feature documents. For a listing of these documents, refer to Chapter 9, "References."

The AR, AC, SCR, SCF, DA, SCA, and CAR features all use direct signaling provided by TCAP and send queries to retrieve distant line status information. The destination of each query (that is, the Point Code of the office supporting the line) is determined by a GTT at a GTT STP. The far-end switch can also respond to non-GTTs for line status requests.

17.04 The CNAM feature uses TCAP to query an SCP data base to determine the name of a caller associated with the calling party information in an IAM. The destination of the SCP data base associated with the feature is determined by a GTT at the GTT STP.

LASS Data Treatment

17.05 The 1A ESS and 5ESS switch offices that offer LASS features must populate data relating to:

(a) Point Codes or Capability Codes of STPs where LASS GTTs are performed. The example shown in Table 3-AM uses Capability Codes.

(b) The Translation Type assigned to LASS.

(c) The SSN assigned to LASS.

17.06 Table 3-AM shows an example of populating PC values for LASS and SSP/800 functionality in the sample network configuration in Figure 3-1. Refer to "General Requirement Parts" in this chapter and Table 3-AN for guidance in populating this data.

17.07 Other considerations relative to LASS operations are described in the following subsections.

Specific CNAM Data Treatment

17.08 The 1A ESS and 5ESS switches that offer CNAM must populate data relating to:

(1) The PCs or Capability Codes of the STP's where CNAM GTTs are performed.

(2) The Translation Type assigned to CNAM.

(3) The SSN assigned to CNAM.

17.09 The CNAM requires a separate Translation Type. The Translation Type (and address information) is used by the STP to determine the Destination Point Code and SSN of the terminating node.

17.10 For LASS the terminating node is the switch where the DN (address information) resides. For CNAM the destination node is an SCP data base.

17.11 The GTTs for LASS and CNAM may be performed at different STPs. The Capability (Alias Point Code) codes may be different for the two applications.

LASS Functionality

A. Privacy Indicator

17.12 The setting of the privacy indicator, which is contained in the IAM, determines whether or not the calling party's DN is displayed when ICLID or BCLID are activated. Originating customers can prevent the display of its DN by invoking the privacy call capability. This can be accomplished in one of four ways (Table 3-AO):

(1) Invoking privacy on a per-call basis. The LASS customer dials a private call toggle code. The calling party DN for the current call is not displayed if the line is public. In addition, other options/codes exist for name/number privacy:

- NNP—Name/Number Privacy
- NNDA—Name/Number Display Allowed.

(2) Assigning privacy on a per-line basis. This prevents the customer's DN from being displayed on every call. It is possible for a customer with permanently private status to allow display of the DN on a per-call basis. Under this condition, the customer would dial the privacy toggle code.

(3) Assigning privacy on a class of service basis. The access code to "Per-Call Privacy Toggle" can be restricted on a class of service basis (requires special feature CPNPC).

(4) Assigning privacy on a per-office basis. This prevents all DNs supported in an office from being displayed.

17.13 Private Calling Party DNs from the incoming line history structure can be put on a screening list but are not voiced back. The RC commands used to populate privacy settings are summarized below. For the 1A ESS switch, the keyword "PPI" is used in each RC command:

(a) PPI keyword is used without CPNPC

(b) PPIE (Line Privacy) keyword is used with CPNPC

(c) CSPPI (Class of Service Privacy) keyword is used with CPNPC

(d) Keywords values are:

(1) **P**—Private
(2) **X**—Public
(3) **N**—Not Set.

Table 3-AP. RC Views/Functions Where Privacy Indicators are Populated

Indicator Type	1A ESS™ Switch	5ESS® Switch
Per-Office Basis	Office Options Table	View 8.1 View 8.21
Per-Class of Service	RC:CCOL	Screen Index View 4.1 View 8.24
Per-Line Basis	RC:LINE RC:TWOPTY RC:MLHG	View 1.6 View 8.18 View 23.2
Per-Call Toggle Code	RC:GENT(*PACT*)	View 9.2 (PDIT)

B. CNAM Privacy Treatment

17.14 The analog Calling Name Display (CNAM) is a special feature that allows the calling party's name to be displayed on a Customer Premises Equipment (CPE). The CNAM Phase 2 development provides three privacy access codes:

(1) A per-call name privacy toggle
(2) A per-call name/number privacy (NNP) not a toggle
(3) A per-call name/number delivery allowed (NNDA) not a toggle.

17.15 The above access codes are originating features, which are not part of the LASS feature package and do not require the CNAM feature. The privacy status is dictated by dialing one of the Per-Call Name/Number Privacy codes that is sent in the

optional parameter "**generic name**" of the IAM. The optional parameter will only be provided if the originator dials one of the new privacy codes. The CNAM permanent privacy indicator is stored in the CNAM SCP data base.

17.16 If a call with the "generic name" optional parameter tandems through another office, the possibility exists that the parameter will not be passed to the terminating office. Previous to the CNAM Phase 2 development, the "generic name" parameter will be treated as an unknown parameter. The 1A ESS switch will always pass unknown parameters. The "generic name" parameter is an unknown parameter in the 4ESS switch. The 4ESS switch provides options to pass unknown parameters. In the 5ESS switch, all "generic name" parameters will be passed.

17.17 If a terminating 5ESS or 1A ESS switch receives these optional parameters prior to their updating to CNAM Phase 2, the call will be completed but the parameters will be ignored.

C. 1A ESS Switch Privacy Treatment

17.18 For 1AE10 and later generics, privacy can be set on a per-call, per-line basis. The privacy indicator is valid for individual lines, centrex lines, 2-party lines, and multiline hunt groups. Private Branch Exchange (PBX) line originations are always set to private.

17.19 In 1AE10 and later generics, the DN is marked "unavailable" for multiparty lines.

17.20 The default value for the privacy indicator for DNs is "not private". That is, DNs are treated as public unless designated as private.

17.21 The CPNP in generic release 1AE10 and later is an optional special feature that changes the way public/private presentation status of a call is determined. With CPNPC, there are three levels of hierarchy for privacy:

- First Level—Calling Line (DN)
- Second Level—Class of service level
- Third Level—Office level.

⇒ NOTE:
If the Privacy/Public is not specified at one level, the next level is checked.

17.22 The CPNPC also allows the use of the "Per-Call Privacy Toggle" access code to be restricted based on the chart column.

D. 5ESS Switch Privacy Treatment

17.23 For present generic releases, privacy can be set on a per-call, per-line, or per-office basis. If the office treatment level for "DN PRIV" (in RC View 8.1) value is

set to **Y**, all DNs in the office are marked as private unless designated as public. If the "DN PRIV" value is set to **N** (default), privacy features in the office are allowed to work normally. If the whole office is designated as private, privacy (that is, per line or per call) cannot be overridden by a toggle code.

17.24 The CPNP in generic release 5E7 and later is an optional special feature that changes the way public/private presentation status of a call is determined. With CPNPC, there are three levels of hierarchy for privacy:

- First Level — Calling Line (DN)
- Second Level — Class of service level
- Third Level — Office level.

NOTE:
If the Privacy/Public is not specified at one level, the next level is checked.

17.25 In addition to allowing privacy per screening index, the CPNPC special feature extends PCP to coin, Hotel/Motel, Charge-a-Call, and 2-party lines.

17.26 The Limited Intra-Group ICLID (LIGI) feature allows the calling DN to be displayed at the terminating station set when calls originate and terminate within the same centrex group. This feature can be assigned on a per-Switching Module (SM) or office basis.

17.27 The Private Option for Last Incoming Number (POLIN) feature provides a per-office option so that LECs can have the last incoming call considered private in all cases, even if the calling party (or originating office) has not marked the number as private.

Uniqueness Indicator

17.28 The setting of the uniqueness indicator for the originating line determines whether or not the DN provided is the true calling DN. The uniqueness indicator is contained in the IAM for an SS7 call. If a line type is marked "nonunique", AC activation to the line is not permitted. For the 1A ESS switch and 5ESS switch, PBX and 2-party Operator Number Identification (ONI) lines are marked "nonunique".

A. 1A ESS Switch Treatment of Uniqueness

17.29 For 1A ESS switch, an office option exists that allows callback attempts to "nonunique" DNs. The default treatment for this option is to prohibit these AC attempts.

B. 5ESS Switch Treatment of Uniqueness

17.30 A 5ESS switch office option exists that allows AC activation to a "nonunique" DN. Similar to the 1A ESS switch, the default setting results in a denied AC if the DN is "nonunique".

Originating/Terminating Scanning

17.31 For the AR and AC features, a TCAP query is sent to the terminating switch to invoke scanning for busy/idle status of the terminating line. If terminating scanning is invoked, the terminating office performs the scanning. If originating scanning is invoked, the originating office is responsible for the scanning.

A. 1A ESS Switch Considerations for Scanning

17.32 The 1A ESS switch supports originating scanning only. If terminating scanning is requested at a 1A ESS switch office, an error message is sent to the originating switch. For the 1A ESS switch, a request for terminating scanning can be made by an originating (that is, 1A ESS switch) office. This capability is provided by the optional Request for Terminating Scanning (RTS) feature.

B. 5ESS Switch Considerations for Scanning

17.33 The 5ESS switch supports both forms of scanning and recommends terminating scanning for busy/idle status. For more information, refer to the 235-118-series of practices titled, *5ESS Switch, Recent Change Procedures, Menu Mode* listed in Chapter 9. The "SCANMODE" field in the LASS Office Parameters (RC view 8.21) can be set to "ORIG" (for originating scanning) or "TERM" (for terminating scanning). The default value is "TERM".

Inter-LATA LASS

A. 1A ESS Switch

17.34 For the 1A ESS switch, the Inter-LATA Calling Party Number/Billing Number (CPN/BN) Delivery and Related Services Feature (CPNBND) provides control over the inter-LATA functionality of the AR/AC features and Screening features. The CPNBND feature is in feature group "9SCNBN." If CPNBND is not loaded, inter-LATA TCAP queries are allowed.

17.35 The blocking of the TCAP queries is divided into two components, AR/AC queries and Screen List Editing (SLE) queries and controlled by bits in the office option table. Word 10, bit 8 of the office options table defines the inter-LATA SLE blocking option. This blocking option allows a 1A ESS switch to prevent

sending the TCAP query message for status information of inter-LATA numbers. The default is "0" which blocks the TCAP query message. Word 10, bit 9 of the office options table defines the inter-LATA AR/AC blocking option. This blocking option allows a 1A ESS switch to prevent sending the TCAP query message for status information for inter-LATA numbers. The default is "0" which blocks the TCAP query message.

B. 5ESS Switch

17.36 For the 5ESS switch, two items exist for the blocking of inter-LATA LASS requests. They are located on RC view 8.21 items "INTER-LATA SCREENING" and "INTER-LATA AR/AC." The value "Y" **allows** inter-LATA screening and AR/AC requests. The value "N" **disallows** inter-LATA screening and AR/AC requests. The default value is "N".

C. Network

17.37 Currently, the issue of inter-LATA TCAP messages is being resolved and there are no specifications available which provide instructions on how to route inter-LATA TCAP messages for LASS (neither the query messages nor the response messages). If inter-LATA TCAP messages are not blocked, an inter-LATA TCAP message will be sent from the originating office, but it may not be possible to deliver it to its destination; or for the destination to correctly deliver the response back to the originating office.

LASS Feature During an NPA Split

17.38 The LASS features rely on ten digits for Directory Number (DN) identification. During a Numbering Plan Area (NPA) split, there is a time interval when two 10-digit numbers represent the same DN. During this time interval, certain LASS features may not operate properly.

17.39 During an NPA split, there is a permissive dialing interval that a DN can be reached using the old dialing plan or the new dialing plan. Before the permissive dialing period, all the offices in an affected area must be preconditioned to handle the new dialing plan. Typically all these offices are not preconditioned simultaneously but in stages. When an office receives a new NPA, the home NPA must be changed in the office for the 5ESS switch and in the rate center for the 1A ESS switch, as part of the preconditioning treatment. These NPAs can also be overwritten by conflict tables in the 1A ESS switch, and LDIT in the 5ESS switch.

17.40 When the home NPA is changed in an originating office, the new NPA is used as part of the calling party number in the IAM. The Calling Party Number (CPN) is used by Automatic Callback (AC), CNAM, and the screening features. Under certain conditions, the new NPA can also be used as part of the CPN for Automatic Recall (AR) TCAP queries, and SLE DN verification TCAP queries.

17.41 Prior to any change in an end office, the STPs must be modified for GTT request, for LASS, and CNAM using the new NPA. The SCP data base for CNAM must also be modified for the new NPA.

17.42 When an AR request is dialed, a digit analysis is done to determine if the last called DN terminates in the local office. If the DN does not terminate in the local office, a TCAP GTT is sent to the STP to determine the status of the DN. If the original call was dialed as seven digits, the NPA must be derived for both the address information field of the GTT and CPN. In the 1A ESS switch, the originators rate center is used, modified by conflict tables. In the 5ESS switch, the originating office NPA is used, modified by LDIT. If the terminating office has not been preconditioned for the new NPA, or the office will remain in the old NPA after the split, the request may fail. (The 5ESS switch compares all ten digits and the response will fail. The 1A ESS switch compares seven digits and will return a response.)

17.43 Before a DN is added to a screening list, it is verified (5ESS switch option) to determine that it is a valid DN. If the DN was dialed as a 7-digit number, the above AR scenario applies and the verification will fail.

17.44 The AC relies on the last incoming call information stored in a line history block. When an AC request is dialed, a digit analysis is performed on the digits in the line history block. If the new NPA was used in the IAM from a preconditioned office, a digit analysis must exist for the new NPA in the office performing the AC. This is required for both the TCAP query and call completion.

17.45 When a DN is placed on a screening list, it is stored as a 10-digit number. When a call is received, the 10-digit calling party information is compared with the DNs on the screening lists to determine if they are to receive screening treatment. If a number were placed on the screening list prior to preconditioning of the NPAs, the number will not match after the calling party office is preconditioned and appropriate screening will not occur.

NOTE:
The 5ESS switch choke list will also be affected by the NPA split.

17.46 The 5ESS switch and the 1A ESS switch provide an optional LASS NPA split feature. This feature will allow the LASS features to continue to operate (from an end user's perspective) as if splitting NPA did not occur. Operating as a single NPA will not restrict the customer from using the old dialing plan or the new dialing plan, until the NPA split controls are removed. After the permissive dialing period, numbers on the screening list will have to be permanently updated.

LASS Network Engineering

17.47 In order to provide consistency in a LASS network, certain office parameters should be applied throughout the network. The 1A ESS and 5ESS switches apply office parameters via different methods and sometimes the correlation of features to different office types is not obvious.

17.48 Table 3-AP and Table 3-AQ show fields that can be applied consistently in the LASS network. Detailed information for these fields and all LASS population rules can be found in COEES index 38 for 1A ESS switches and 235-190-130 (Local Area Signaling Services) for 5ESS switches.

Table 3-AQ. Consistency in AR/AC Data Values

Item	1A ESS™ Switch, Set Card	5ESS® Switch, Form 5945, RC View 8.1
Number of (active) AR request blocks if AR is separate. If not separate, AR/AC request blocks.	LARBLK range=10 to 512, and 0	Fixed at 12 per customer, 128 per SM.
Number concurrent (active) AC request blocks	LACBLK range=10 to 512, and 0	See above.
Amount of time for scanning before the first ringback attempt.	LASTRB range = 1 to 6, corresponding to 45 to 120 seconds in 15-second increments default= 2 (60 seconds)	FIELD= B/I SCAN range = 45 to 120 seconds default= 60 seconds
Amount of time for scanning if the ringback goes unanswered and continues until time out or the ring back is answered.	LARBST range = 1 to 37, corresponding to 3 to 12 minutes in 15-second increments default = 9 (5 minutes)	FIELD= RNGBK WAIT range=3 to 12 minutes default = 5 minutes
Total amount of time delayed processing will check for each activation.	LARTIM range = 1 to 30, corresponding to 16 to 45 minutes in 1-minute increments default= 15 (30 minutes)	FIELD= TIMEOUT range=15 to 45 minutes default = 30 minutes
Defines the max. number of ringback attempts given a customer, per activation request.	LARBNM range=1 to 12 ringbacks default=1 ringback	FIELD= MAX RNGBK range=1 to 12 ringbacks default=1 ringback
Defines the number of ring cycles in ringback sequence.	LARBCC range = 1 to 6, corresponding to 2 to 7 cycles default=3 (4 cycles)	FIELD= RNG CYCLE range=2 to 7 cycles default= 4 cycles

Table 3-AR. Consistency In Screening Data Values

Item	1A ESS™ Switch, Set Card	5ESS® Switch, Form 5945, RC View 8.1
Max. number of entries on an SCR list	LASCRE range = 3 to 31 default = 3	FIELD=SCR MAX SZE range = 3 to 31 default = 6
Max. number of entries on an SCF list	LASCFE range = 3 to 31 default = 3	FIELD=SCF MAX SZE range = 3 to 31 default = 6
Max. number of entries on a DA list	LADAE range = 3 to 31 default = 3	FIELD=SDA MAX SZE range = 3 to 31 default = 6
Max. number of entries on an SCA list	LASCAE range = 3 to 31 default = 3	FIELD=SCA MAX SZE range = 3 to 31 default = 6
Max. number of entries on a CAR list	LACARE range = 3 to 31 default = 3	FIELD=CAR MAX SZE range = 3 to 31 default = 6

18. Advanced Services Platform Specific Requirements

18.01 Advanced Service Platform (ASP) is a service that uses the public switched network to provide private network features and capabilities. The architecture uses intelligent switches equipped with the Service Switching Point (SSP) capabilities, interacting with SCPs for routing and other call handling instructions. This service in the 4ESS switch is referred to as AIN and is compatible with AIN, Release 0.1, TCAP protocol.

18.02 Communication with the SCP(s) is provided by either AIN Release 0 TCAP protocol (Bellcore (TR-TSY-000402) or AIN Release 0.1 TCAP protocol (Bellcore TR-TSY-001284 and TR-TSY-1285). The Network Access Point (NAP) can also be used to provide a more cost-effective, widespread access to ASP features. An ASP architecture overview is shown in Figure 3-9.

18.03 An ASP SSP has the ability to recognize ASP trigger events, suspend normal call processing, and launch a TCAP query to an ASP SCP requesting further instructions on treatment of the call. Based on these instructions, the ASP SSP has the ability to:

(a) If the SCP requests it, play announcements and collect more digits

(b) Incorporate network management controls (for example, automatic call gapping of ASP calls)

(c) Route the call over private or public facilities.

18.04 An ASP NAP has the ability to recognize ASP trigger events, but rather than launch a query to an ASP SCP, it uses modified EAMF or SS7 signaling to route the call to an ASP SSP which in turn communicates with the SCP.

NOTE:
If SS7 signaling is used to route the call, data population and consistency should follow the guidelines described in this section.

18.05 General descriptions of the ASP feature can be found in Bellcore TR-TSY-000402, *Additional Service Switching Point and Related End Office Capabilities* (Including Private Virtual Network Services). AIN 0.1 protocol is described in TR-TSY-001284, "Advanced Intelligent Network (AIN) 0.1 Switching Systems Generic Requirements", and in TR-TSY-001285, "AIN 0.1 Switch - Service Control Point (SCP) Applications Protocol Interface - Generic Requirements". A more detailed description of the 5ESS switch feature for ASP can be found in 235-190-125, *5ESS Switch, Advanced Services Platform Feature Document.* A description of the 1A ESS switch feature for ASP can be found in 231-390-519, *Advanced Services Platform/Service Switching Point (ASP/SSP) Feature Document,* and 256-030-100, *Advanced Services Platform Network Architecture and Services Consideration Guide.*

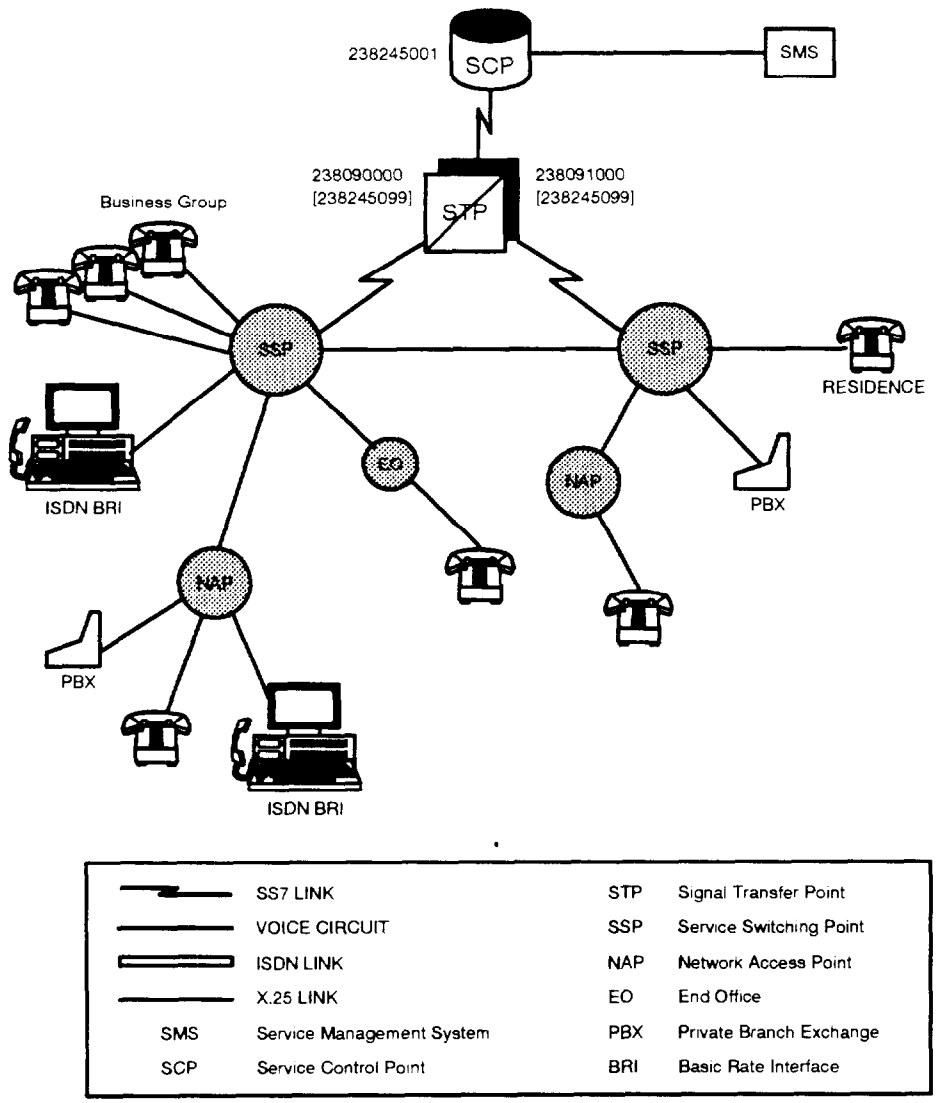


Figure 3-9. ASP Architecture Overview

5ESS Switch Specific Feature Description

18.06 The 5ESS switch may assume either the ASP SSP or NAP roles.

A. ASP Network Access Point Functionality

18.07 The 5ESS switch ASP NAP allows access to ASP data base services by connectivity with an ASP SSP office through SS7 or modified EAMF signaling in 5E6(1) and later generics.

18.08 A 5ESS switch configured as an ASP NAP office must populate the following network data:

(a) The carrier identifier that is to be outpulsed in the NAP Equal Access signaling stream to the ASP SSP. The carrier identifier must be defined as a **pseudo** carrier.

(b) The ASP ANI information digits outpulsed in the NAP to SSP Equal Access signaling stream indicating an ASP call.

18.09 For guidance in populating ASP data items a-b, refer to 235-190-125, *5ESS Switch ASP Feature Document.*

B. ASP SSP Functionality

18.10 The 5ESS switch ASP SSP functionality is introduced in 5E6(1) and later generics.

18.11 A 5ESS switch configured as an ASP SSP (Table 3-AR) office must populate the following network data:

(a) The Point Codes or Capability Code of the STPs where Global Title Translations are performed.

(b) The Translation Type assigned to ASP.

(c) The Subsystem Number assigned to ASP.

(d) The cluster value of the ASP SCP data base.

(e) The SCP Response Timer for ASP service. This is the number of seconds an ASP call waits for a response to an SCP query.

(f) The default line Digital Analysis Selector (DAS) used for retranslating ASP calls after querying an SCP and receiving a response to route via the LEC.

(g) The default trunk DAS used for retranslating ASP calls after querying an SCP and receiving a response to route via the LEC.

(h) The carrier identifier that is to be outpulsed in the NAP Equal Access signaling stream to the ASP SSP. The carrier identifier must be defined as a pseudo carrier.

(i) The ASP ANI information digits outpulsed in the NAP to SSP Equal Access signaling stream indicating an ASP call.

(j) Announcement Codes returned from the SCP for specific ASP announcements.

(k) Billing Indicator returned from the SCP if the ASP call is to be billed at the ASP SSP.

18.12 For guidance in populating ASP data items a through d, refer to "General Data Requirements", Tables 3-AN and 3-AP. For items e through k, refer to 235-190-125 *5ESS Switch ASP Feature Document.*

Table 3-AS. Example Point Code Information for ASP Functionality

Signaling Point	ASP GTT STPs	SCP Cluster
5ESS® Switch ASP SSP	PC1 = 238245099 PC2 = 238245099	245

NOTE:
This example assumes Capability Codes are used for GT routing.

C. 4ESS Switch Specific Feature Description

18.13 The 4ESS switch AIN SSP functionality is introduced in 4E18 and later generics. The capabilities provided by this feature are a subset of AIN triggers (Trunk and DNT) and announcement capabilities [Service Circuit Switch (SCS) functionality] as defined in Bellcore's Specifications AIN 0.1 TR-NWT-001284 and TR-NWT-001285. For specific details, refer to 234-090-0019.

18.14 A 4ESS switch configured as an SSP office must populate the following feature data:

(a) The Point Codes or Capability Code of the STPs where Global Title Translations are performed

(b) The Translation Type assigned to AIN.

(c) The Subsystem Number assigned to AIN

(d) The cluster value of the AIN SCP data base

(e) The SCP Response Timer for AIN service. This is the number of seconds an AIN call waits for a response to an SCP query

(f) The Code Grouping Recent Changes for the triggers on the trunks or Called Numbers.

19. SSP/800 Specific Requirements

19.01 The SSP/800 allows end, tandem, or access tandem switching offices to interface with an SCP for implementing 800 Number Services. The interface is provided by TCAP, using the SCCP protocol.

19.02 A 5ESS switch feature description for SSP/800 can be found in 235-190-120, *5ESS Switch, Common Channel Signaling Services Features.* A 1A ESS switch feature description for SSP/800 can be found in 231-390-509, *Service Switching Point, Common Channel Signaling System 7, Feature Document, 1A ESS Switch,* and 231-390-510, *800 Service, Common Channel Signaling System 7, Feature Document, 1A ESS Switch.* A 4ESS switch reference to 800 services can be found in 234-090-002, *4ESS Feature Document Service Switching Point - 800.*

19.03 When an SSP/800 message is sent to the SCP, routing instructions are returned from the SCP for subsequent handling of the signaling message. Note that the routing data returned must be routable from the SSP switch.

19.04 The 1A ESS, 4ESS, and 5ESS switch offices that offer SSP/800 service must populate data relating to the following:

(a) The Point Codes or Capability Code of the STPs where SSP/800 GTTs are performed.

(b) The Translation Type assigned to SSP/800

(c) The Subsystem Number assigned to SSP/800

(d) The cluster value of the SCP data base.

19.05 Note that the SSP/800 test can provide verification of SSP/800 related data. For additional information, refer to Chapter 6, "Tools."

19.06 Additional features are required to support other toll free service access codes such as 888.

20. OSPS Specific Requirements

20.01 The Operator Services Position System (OSPS), in 5E5 and later generics, uses SS7 capabilities in two of its features: Billed Number Screening and Calling Card Verification. In Billed Number Screening, a TCAP query is sent to a Line Information Data Base (LIDB) to verify whether or not a Directory Number can be billed as a collect or third party number. In Calling Card Verification, a TCAP query is also sent to a LIDB; however, the query is to validate a calling card number and personal identification number entered by a customer or operator. Additional details on the SS7 interface with these two features can be found in 235-190-120, *5ESS Switch Common Channel Signaling Services Features.*

20.02 The 5ESS switch offices that support Billed Number Screening and Calling Card Verification must populate data relating to the following:

(a) The Point Codes or Capability Code of the STPs where Global Title Translations are performed

(b) The Translation Types assigned to Billed Number Screening and Calling Card Verification (one Type assigned to each)

(c) The Subsystem Numbers assigned to Billed Number Screening and Calling Card Verification (one SSN assigned to each)

(d) The cluster value of the LIDB data base.

Maintenance Procedures

4

Contents

Contents Page

Contents Page

Contents Page

Maintenance Procedures

4

1. Signaling Link Trouble

Detecting Signaling Link Trouble

1.01 Loss of Signaling Links (SLKs) and/or service could be caused by any one of the following:

(a) Faulty transmission facilities

(b) Faulty signaling link hardware at the near-end and/or far-end

(c) Link node sanity failure

(d) Link node transmit buffer congestion

(e) Periodic signaling link test failure.

1.02 Figure 4-1 presents the basic flow of events and critical event messages that are reported, during a signaling link failure.

1.03 In the event that a signaling link is declared failed and diagnostics resolve the problem, the link is put back into service. However, if diagnostics are unable to resolve the failure, manual intervention is required (see Figure 4-2). For information on troubleshooting the problem, refer to "Procedures for Isolating SLK Trouble" in this chapter.

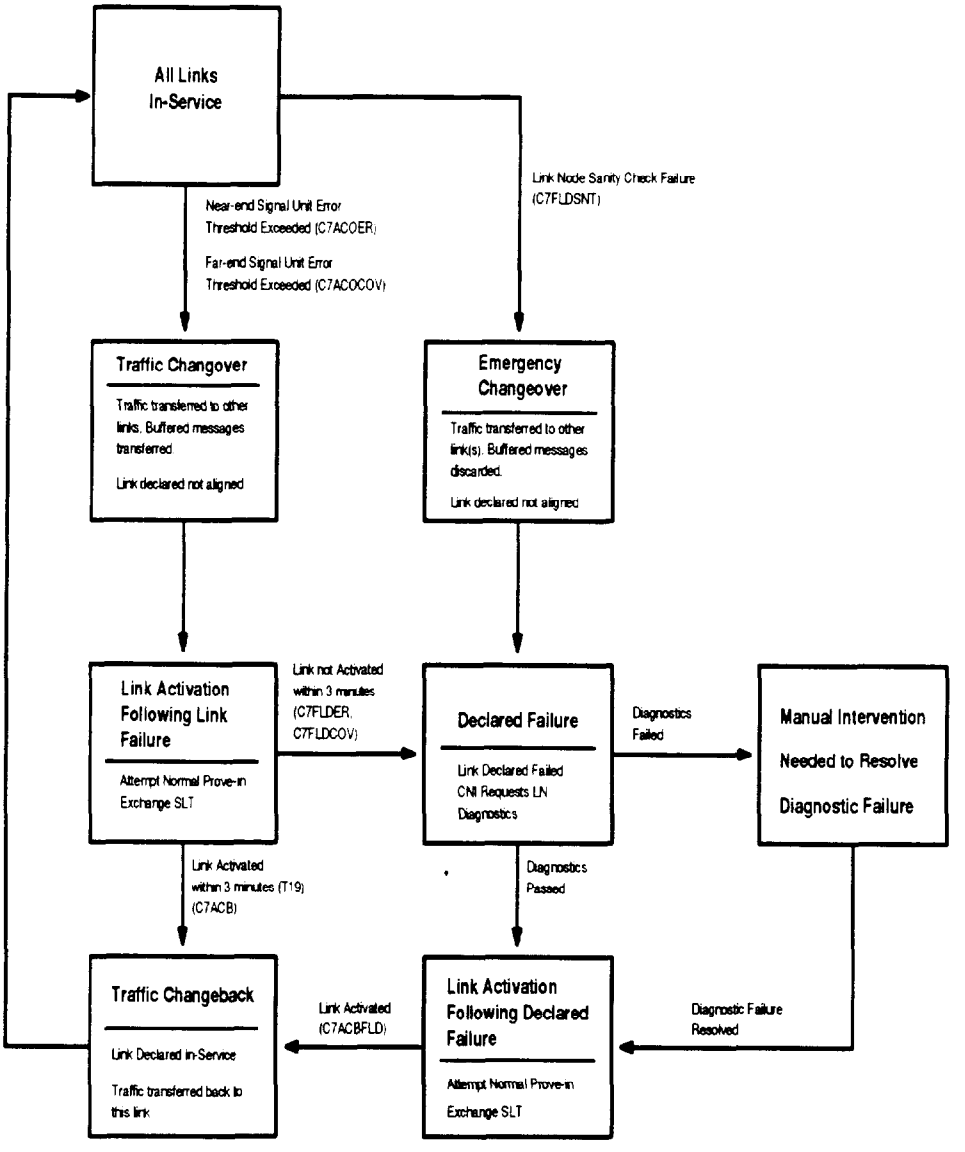


Figure 4-1. Signaling Link Failure Reports

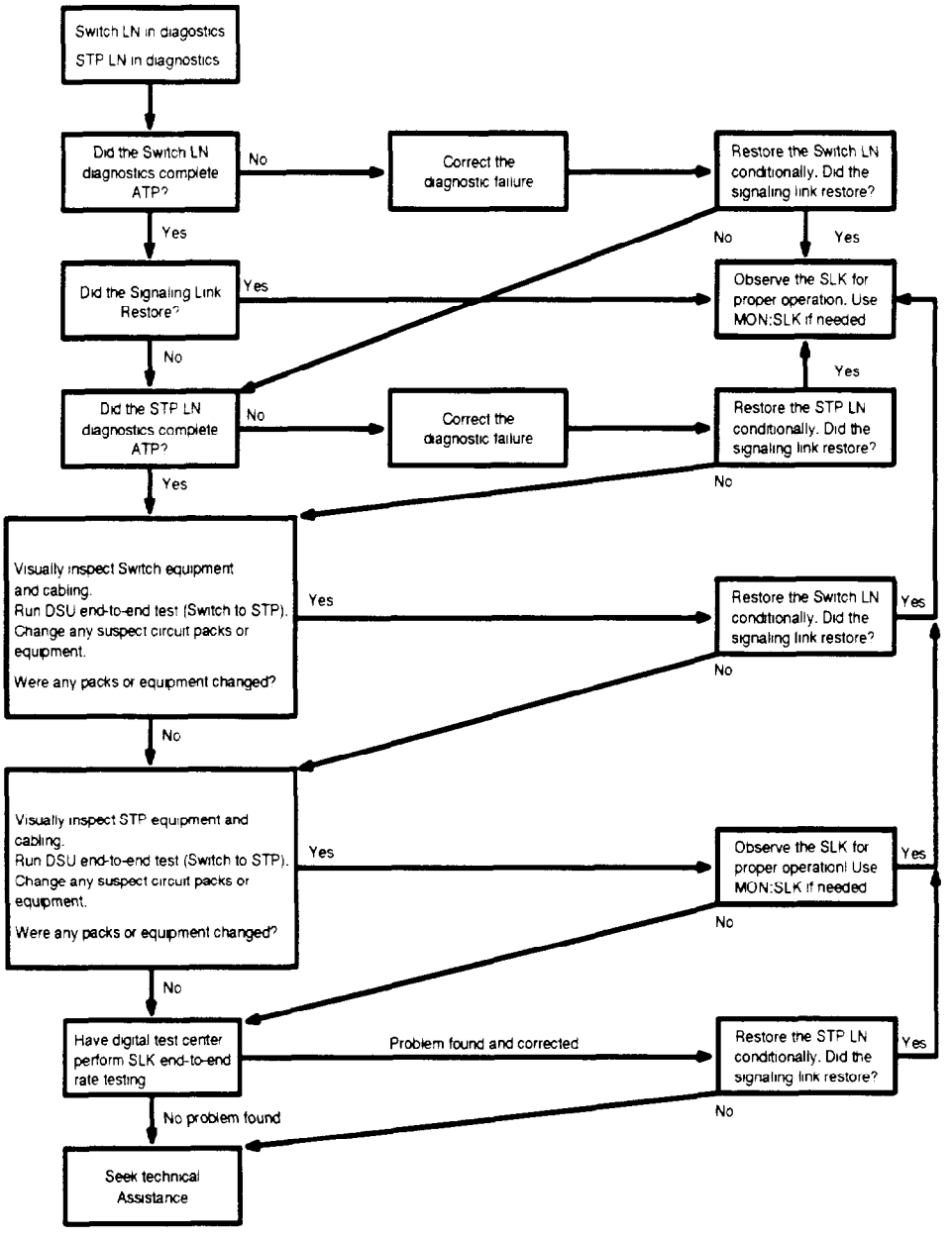


Figure 4-2. Recovery from Declared Link Failure

A. Faulty Transmission Facilities

1.04 Loss of transmission facilities can be serious, but occasional glitches or carrier fades are not uncommon. A failure of less than 3 minutes for one signaling link results in the temporary transfer of traffic to the available signaling link(s). This is evidenced by the following sequence of **REPT CNCE** critical event messages:

- **C7ACOER** (if the near-end signal unit error threshold is exceeded) or **C7ACOCOV** (if the far-end signal unit error threshold is exceeded)
- **C7LSF** (if all links are down in the linkset)
- **C7ACB** (automatic changeback from a failure that is not a declared failure)
- **C7LSFE** (if one of the links in the linkset becomes available).

1.05 A failure greater than timer T19 in the Common Network Interface (CNI) file (default time is 3 minutes) causes both ends of the signaling link to diagnose the signaling link hardware. Assuming no problems are found and the facilities are normal at the conclusion of diagnostics, the SLK is restored and traffic transferred back to it. This is evidenced by the following sequence of **REPT CNCE** critical event messages:

- **C7ACOER** (if the near-end signal unit error threshold is exceeded) or **C7ACOCOV** (if the far-end signal unit error threshold is exceeded)
- **C7LSF** (if all links are down in the linkset)
- **C7FLDER** (if the near-end is declaring the failure) or **C7FLDCOV** (if the far-end is declaring the failure)
- **C7ACBFLD** (automatic changeback from a declared failure)
- **C7LSFE** (if one of the links in the linkset becomes available).

If the other links encounter trouble while one link is being diagnosed, resulting in no available SLKs, the link diagnostics are aborted and both SLKs try to establish themselves on an emergency basis. If both (or all) of the SLKs are common to some transmission facilities, a facility failure results in a loss of service, as no alternate links are available to change traffic over to.

B. Faulty Signaling Link Hardware at the Near-End and/or Far-End

1.06 When signaling link hardware, either at the near-end or far-end, is causing signal units to be in error, the signaling link error threshold is exceeded. A hardware failure results in a declared failure which in turn causes both ends to run diagnostics on the signaling link hardware. A critical event scenario analogous to that described on page 4-4 can be found on the Receive-Only Printer (ROP).

Marginal performance or intermittent failures are more difficult to resolve. The Thirty Minute Marginal Performance Report is useful in analyzing these types of problems.

The Signaling Network Performance Reports (Parts 1 and 2) are helpful in observing long-term trends.

C. Link Node Sanity Failure

1.07 A signaling link may fail if the link node hardware declares itself insane. In this case, traffic changes over to the other link(s), but untransmitted, buffered messages are lost. Critical event **C7FLDSNT** would appear on the ROP and all traffic on the affected signaling link would undergo an emergency changeover to the available signaling link(s). The link node would undergo a series of diagnostics to try to correct the problem. On successful completion of the diagnostics, the link would be activated and critical event **C7ACBFLD** would be reported on the ROP. The signaling link would be put back into service and traffic transferred back to it.

D. Link Node Transmit Buffer Congestion

1.08 A signaling link may experience transmit buffer congestion if the far-end is having trouble receiving messages. A discard and throttling strategy is used depending on the level of congestion. Messages are discarded at some of the congestion levels. This condition is usually a result of a far-end problem. The **REPT CNCE** critical events **C7LCON1X**, **C7LCON2X**, and **C7LCON3X** inform the office of the congestion level reached (1, 2, or 3, respectively). The **REPT CNCE** critical events **C7LCDIS1X**, **C7LCDIS2X**, and **C7LCDIS3X** inform the office that congestion discard Levels 1, 2, and 3 (respectively) have been reached. Service indicators also report when a link is in congestion.

The **REPT CNCE** critical events **C7LCABM1X**, **C7LCABM2X**, and **C7LCABM3X** inform the office that buffer occupancy has dropped below abatement threshold. If congestion remains at any one level for more than 30 seconds, then the link is removed from service, accompanied by a **RING REPORT CNCE** report.

E. Periodic Signaling Link Test Failure

1.09 The Signaling Link Test (SLT) is defined in the American National Standards Institute (ANSI) SS7 protocol standards (T1.111.7.-1988 Section 2.2) and in Bellcore TR-NWT-000246, *Bell Communications Research Specification of Signaling System Number 7*, Section Q.707. The SLT is performed during an SLK activation and also periodically once the SLK has been activated.

Following an SLK activation, the Periodic SLT (PSLT) exchange begins between the near-end and far-end of the SLK.

NOTE:
Lucent Technologies currently provides a 5-minute interval immediately following SLK activation before execution of the PSLT is allowed to begin. This interval is intended to provide time for a craftsperson or Operation Support System to inhibit the PSLT (if desired).

1.10 The PSLT performed on one SLK is independent of the tests performed on the other in-service SLKs. The following PSLT exchange is initiated periodically for each in-service SLK, based on the value of the T1.111.7-T2 timer.

- The Signaling System 7 (SS7) link node sends a Signaling Link Test Message (SLTM) to the far-end of the SLK and waits for a correct Signaling Link Test Acknowledgement (SLTA) from the far-end.

  NOTE:
  The SLTMs being sent are placed in the link node transmit buffer. If this buffer is congested, the PSLT will not be run until the congestion abates. If an SLTM arrives when the transmit buffer is congested, it will be acknowledged (SLTA) regardless of transmit buffer congestion.

1.11 An acknowledgement supervision timer (T1.111.7-T1) is started when the SLTM is sent.

NOTE:
Lucent Technologies implements a default value of 10 seconds.

(a) A received SLTA shall be deemed correct if all of the following conditions are satisfied:

— The SLTA was received on the SLK to which the SLT applies.

— The signaling link code field in the SLTA identifies the physical SLK to which the SLT applies.

— The Originating Point Code (OPC) in the SLTA identifies the signaling point at the far-end of the SLK.

— The Destination Point Code (DPC) in the SLTA identifies the signaling point at the near-end of the SLK (that is, the signaling point that has initiated the SLT).

— The contents of the Test Pattern field in the SLTA are the same as the contents of the Test Pattern field in the SLTM previously sent.

1.12 If a correct SLTA is received before the T1.111.7-T1 (T1) timer has expired, the SLT has *passed* and the SLK remains in-service.

(a) If an incorrect SLTA is received, it is ignored and the T1 timer will continue to run. If the T1 timer expires before a correct SLTA is received from the remote end, one of two actions will be taken:

— If only one SLTM has been sent for this SLT, another SLTM is sent and the T1 timer is restarted.

— If two SLTMs have been sent for this SLT, the SLT has *failed*. The following action is taken:

(1) The SLK is forced Out-Of-Service (OOS) at Level 2.

(2) Existing message traffic, if any, is routed from the now OOS SLK to an alternate SLK.

(3) **REPT CNCE** critical event C7FLDSNT (with a failure code of [hexadecimal] 606) is reported.

(4) An attempt is made to bring the SLK back into service. An SLT must be passed in order for the SLK to be restored to in-service.

(5) If the SLK is not activated within 3 minutes, the SLK is declared failed and diagnostics are requested on the SLK's link node. If the diagnostics pass, normal SLK prove-in is again attempted. If diagnostics fail, manual intervention is needed to resolve the failure.

NOTE:
Forcing an SLK OOS in response to an SLT failure may create a Signaling Point Isolation (SPI) condition. If this happens, Emergency Restart procedures, rather than normal restoral procedures, shall be used to attempt to bring the forced OOS SLK back into service. Nevertheless, one of the conditions necessary to restoring the SLK to in-service shall be that an SLT be successfully executed on that SLK.

1.13 Since PSLT has the capability of removing in-service SLKs, the following input message (Table 4-A) has been provided to inhibit, allow, or print the status of PSLT for one or more SLKs:

Table 4-A. Signaling Link Test Messages

Application	Input Message
1A ESS™ Switch	INH:PSLT { ALL I (*a*,*b*) }; *c*
4ESS™ Switch	INH:PSLT { ALL I (*a*,*b*) }; *c*
5ESS® Switch	INH:PSLT={ ALL I *a*-*b* }: *c*
A-I-Net® STP	INH:PSLT={ ALL I DOM I *a*-*b* }: *c*

where: *a* = SLK group number
b = SLK member number
c = ON, OFF, or STATUS

Note:
The message must be entered at both ends of the PSLT SLK.

1.14 To inhibit the PSLT for one or more SLKs, enter the **ON** keyword. To allow the PSLT for one or more SLKs, enter the **OFF** keyword. To print the SLKs that have PSLT inhibited, enter the **STATUS** keyword. For more details, refer to the appropriate application's input manual.

NOTE:
This inhibit is only for the periodic SLT. The SLT performed during link activation cannot be inhibited.

Procedures for Isolating SLK Trouble

1.15 When a signaling link fails to go into service, the problem can be isolated in a few steps. Verify the following prerequisites are met when trying to activate an SLK:

(a) The switch and *A-I-Net*® advanced intelligent network products Signal Transfer Point (STP) link nodes successfully pass diagnostics and are in the active (ACT) state.

(b) The switch and STP SLK data bases recognize the SLK as available.

(c) The Digital Service Unit (DSU) options (explained in Chapter 2, "Link and Facility Activation Procedures") are properly set at both ends of the SLK.

1.16 No manual loops on the DSU should be in effect at either end. The front of the Lucent Technologies 2556 DSU should appear as shown in Figure 4-3.

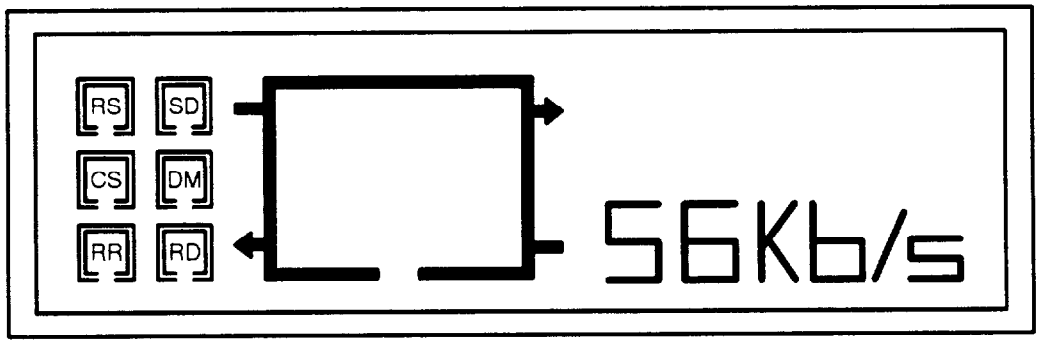


Figure 4-3. Front Display of the Lucent Technologies 2556 DSU Under Normal Operation

1.17 Signaling link SS7 protocol Levels 2 and 3 messages incoming to the switch or *A-I-Net* products STP should be monitored using the **MON:SLK** input message. This tool should be activated at the switch and *A-I-Net* products STP. Signaling link activation trouble can be categorized into three types of problems:

(a) No Signaling Link Connectivity

(b) Prove-In Failure

(c) Successful Prove-In Followed by an SLT Failure.

A. No Signaling Link Connectivity

1.18 When no signaling link connectivity exists, the following procedure should be used to isolate the problem.

(1) Run the DSU end-to-end tests from each end of the SLK. These procedures are found under the heading "Digital Service Unit (DSU) End-to-End Testing" later in this chapter. Potential error sources include incorrect facility wiring or a defective channel bank. Any failures are to be resolved.

(2) At the switch's Digital Facility Access (DFA) frame/cabinet, activate local loopback in the DSU. The front of the Lucent Technologies 2556 DSU should look like Figure 4-4. If proper connectivity exists between the CNI ring and the DFA frame/cabinet, SLK monitoring should indicate a successful prove-in followed by an SLT failure. If prove-in is not attempted, the connectivity problem lies in the switch between the CNI link node and the DFA frame/cabinet. Potential error sources include the wrong cable being used or the cable not being properly connected. Any problems found should be corrected.

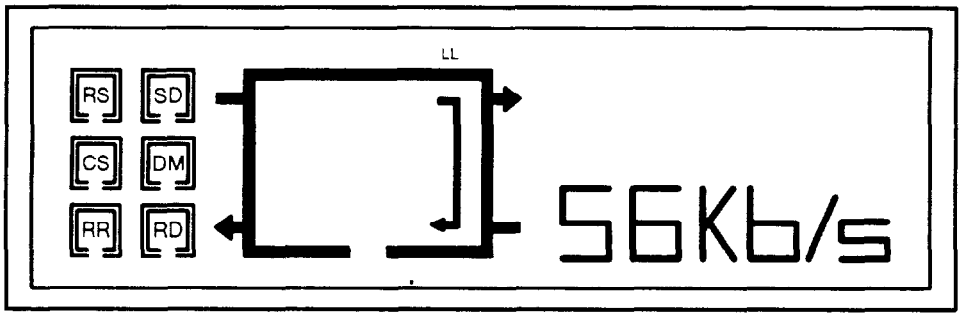


Figure 4-4. Front Display of the Lucent Technologies 2556 DSU With Local Loopback

(3) Remove the local loopback in the switch's DSU.

NOTE:
Refer to Dataphone® II, 2500-series User's Manual for switch option settings and functions.

(4) Set up a digital loopback at the far-end STP's DSU. If the STP is using a Lucent Technologies 2556 DSU, this is accomplished by pressing the DL button on the STP's DSU. The front of the Lucent Technologies 2556 DSU should look like Figure 4-5.

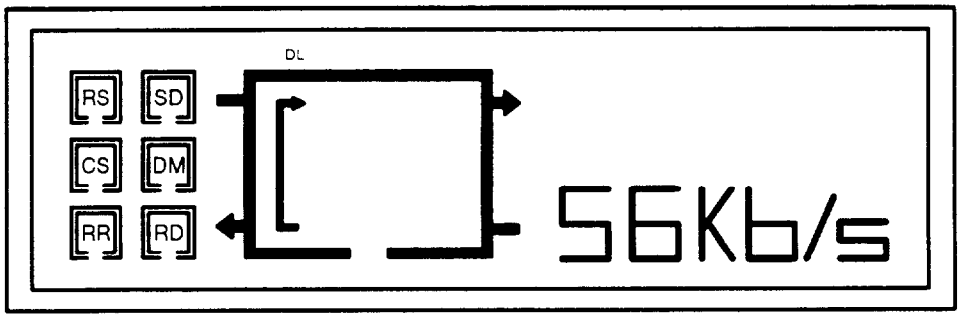


Figure 4-5. Front Display of the Lucent Technologies 2556 DSU with Digital Loopback

If the STP is using the *Datatel** DCP3189 DSU, the digital loopback is accomplished by pressing the Remote Digital Loopback (RDL) button on the STP's DSU.

If connectivity exists from the CNI link node in the switch to the DFA frame/cabinet at the far-end STP, SLK monitoring shows a successful prove-in (up through Level 2) followed by an SLT failure. If prove-in is not attempted, the connectivity problem lies in the facilities between the switch's DFA frame/cabinet and the STP's DSU.

(5) Repeat Steps 2 through 4, but this time test from the STP end. Any failure found is to be resolved.

* Registered trademark of Lenkurt Inc.

B. Prove-In Failure

1.19 If prove-in fails during signaling link establishment, this indicates that error checks detected too many errors in the signal units being sent. This could be an indication of poor facilities between the switch and STP, or it could be faulty SLK hardware at either end of the signaling link. A typical prove-in failure as seen by SLK monitoring shows the following **MON:SLK** sequence:

- **ALIGNMENT NOT POSSIBLE, T2 EXPIRED**
- **ALIGNMENT ERROR RATE THRESHOLD EXCEEDED.**

1.20 To isolate a prove-in failure, perform the following:

(1) Run the DSU end-to-end tests from each end of the SLK. Again, these procedures are found later in paragraph 1.26. Any failures found are to be resolved.

(2) At the switch's DFA frame/cabinet, activate a local loopback on the DSU. If good hardware exists from the CNI link node to the DFA DSU, SLK monitoring shows a successful prove-in (up through Level 2) followed by an SLT failure. If the prove-in fails, the problem exists in one of three places:

- The SLK hardware in the Link Node
- The cable connecting the Link Node to the DSU
- The SLK hardware in the DSU.

⇒ NOTE:
Run Link Node diagnostics to help isolate the problem. Replace hardware as necessary to resolve any failures.

(3) Remove the local loopback in the switch's DSU.

(4) Activate a digital loopback at the far-end STP's DSU. If good hardware exists from the switch's CNI link node to the far-end STP's DSU, SLK monitoring shows a successful prove-in followed by an SLT failure. If prove-in fails, the problem lies in the facilities between the switch's DFA frame/cabinet and the STP's DSU.

(5) Repeat Steps 2 through 4, but this time test from the STP end. Any failure found is to be resolved.

C. Successful Prove-In Followed by Signaling Link Test Failure

1.21 If prove-in passes but the SLT exchange fails, there is a data base mismatch between the switch and the STP. The SLT exchange is a verification of the switch's point code, the STP's point code, the signaling link code/linkset member, and a test pattern. It may be sent by either end (switch or STP). An SLTA is returned to the SLT sender if the receiving office agrees with the translations in the SLT. If the SLT translations are not agreed on by the receiving office, two events occur:

(a) The office that received the SLT fails to acknowledge the SLT (that is, no SLTA is sent).

(b) The office that sent the SLT experiences an SLTA timer expiration.

1.22 In the event of SLT failure, SLK monitoring prints one of two (or both) messages depending on which end of the SLT exchange is being monitored. The office that receives an SLT and finds the data base mismatch prints a message (REPT SLT) indicating that the SLT is not being acknowledged and indicates the element that does not match. The office that sent the SLT prints a message (REPT SLT) indicating that the SLTA timer has expired.

1.23 There are two prominent causes of SLT failures:

(a) An incorrect signaling link code/linkset member

(b) An incorrect point code stored in link translations.

1.24 Resolving SLT failures is simply a matter of determining which end has the incorrect translations and correcting the translations in the data base. For assistance in determining the correct translations, refer to Chapter 3, "Data Administration Guidelines" for additional information.

Digital Service Unit End-to-End Testing

1.25 The following sections describe the steps needed to perform DSU end-to-end testing. Two DSU types are mentioned: the Lucent Technologies 2556 and the *Datatel*® DCP3189.

A. Lucent Technologies 2556 DSU to Lucent Technologies 2556 DSU

1.26 This section provides end-to-end testing procedures from the Lucent Technologies 2556 DSU to the Lucent Technologies 2556 DSU. The test requires one operator.

(1) At the near-end DSU, press the **RL** button. This actives a digital loopback condition at the far-end DSU.

(2) At the near-end DSU, press the **TP** button. This sends a test signal through the loopback at the far-end DSU.

(3) "**ERROR**" flashes on the display panel of the near-end DSU if the test fails. No message is displayed if the test is successful.

(4) Testing is complete. It is considered successful if the above scenario is followed. Otherwise, appropriate corrective actions are required.

(5) To restore the DSUs to their pretest state, press the buttons again in reverse order. First release the **TP** button and then release the **RL** button. Thirty seconds are required for the DSUs to return to normal.

B. Lucent Technologies 2556 DSU to *Datatel*® DCP3189 DSU

1.27 This section provides end-to-end testing procedures from the Lucent Technologies 2556 DSU to the *Datatel* DCP3189 DSU. The test requires two operators.

(1) Press the **RL** button on the Lucent Technologies 2556 DSU. There is no visible effect at either end.

(2) Press the **TP** button in addition to the **RL** button. The **CMP** lamp on the *Datatel* DSU should light 5 seconds after completion of the previous step.

(3) At the *Datatel* DSU, press the **LDL** button to activate local digital loopback.

(4) Flashing "**ERROR**" display disappears on the Lucent Technologies 2556 DSU display panel.

(5) Testing is complete. It is considered successful if the above scenario is followed. Otherwise, appropriate corrective actions are required.

(6) To restore the DSUs to their pretest state, press the **TP** and **RL** buttons again on the Lucent Technologies 2556 DSU and the **LDL** button on the *Datatel* DSU.

C. *Datatel* DCP3189 DSU to Lucent Technologies 2556 DSU

1.28 This section provides end-to-end testing procedures from the *Datatel* DCP3189 DSU to the Lucent Technologies 2556 DSU. The test requires two operators.

(1) Press the **RDL** button on the *Datatel* DCP3189 DSU to activate remote digital loopback. The **TST** lamp lights.

(2) Press the **DL** button on the Lucent Technologies 2556 DSU to activate digital loopback.

(3) The **CMP** lamp on the *Datatel* DSU lights 5 seconds after the Lucent Technologies DSU action to confirm reception of loopback signal.

(4) Testing is complete. It is considered successful if the above events have occurred as specified. Otherwise, appropriate corrective actions are required.

(5) To return the DSUs to their pretest state, press the **RDL** and **DL** buttons again on their respective DSUs.

D. *Datatel* DCP3189 DSU to *Datatel* DCP3189 DSU

1.29 This section provides end-to-end testing procedures from the *Datatel* DCP3189 DSU to the *Datatel* DCP3189 DSU. The test requires two operators.

(1) The far-end DSU must be conditioned for testing by enabling **RDL** option. This is achieved by moving switch 2,5 to the "**on**" position. The near-end DSU must move switch 2,5 to the "**off**" position.

(2) At the near-end DSU, pressing the **RDL** button generates a test pattern to be sent to the far-end DSU.

(3) At the far-end DSU, the **CMP** lamp lights 5 seconds after the near-end action to acknowledge reception of the test signal.

(4) At the near-end DSU, the **CMP** lamp lights after an additional 5 seconds to confirm reception of the test signal from the far-end DSU.

(5) The **TST** lamp should light at both DSUs.

(6) Testing is complete. It is considered successful if the above events have occurred as specified. Otherwise, appropriate corrective actions are required.

(7) Restore the far-end DSU to its pretest state by pressing the **RDL** button again. A normal connection resumes 30 seconds later.

2. Initialization

2.01 The CNI software subsystem consists of three components:

(a) The Lucent Technologies 3B20D computer system [*UNIX** Real-Time Reliable (RTR) Operating System]

(b) The Interprocess Message Switch (IMS)

(c) The Common Network Interface (CNI) software.

2.02 Each subsystem performs some share of the functions necessary to keep the SS7 interface operational. *UNIX* RTR Operating System provides a set of procedures that enables users to efficiently share the 3B20D computer and physical resources such as computer time, storage space, and peripheral devices. The IMS system, based on a ring interconnected structure, provides for interprocess communication strategies, the craft interface, hardware maintenance, system initialization, audits, and measurements. The CNI software implements the necessary communication protocol functions which are common to all users interfacing to an SS7 network.

2.03 The CNI and the IMS systems support several various levels of initialization. Each offers a different trade-off between completeness of initialization and impact on the 1A ESS™ switch, 4ESS switch, 5ESS® switch, and *A-I-Net* products STP applications. Both the CNI and IMS systems rely on the escalation from one initialization level to a more severe level as a result of errors.

2.04 Table 4-B provides a cross-reference of craft input messages to their corresponding CNI and IMS level initializations.

* Registered trademark of Novell Inc.

Table 4-B. CNI/IMS Initialization Input Messages

CNI STP Level	IMS Level	1A ESS™ Switch	4ESS™ Switch	5ESS® Switch	*A-I-Net*® STP
0	0	INIT:RING 0	INIT:RING 0	INIT:CNI,LVL0	INIT:STP:LEVEL=0
1	1B	INIT:RING 1	INIT:RING 1	INIT:CNI,LVL1	INIT:STP:LEVEL=1
2	3	INIT:RING 2	INIT:RING 2	INIT:CNI,LVL2	--
3	3	INIT:RING 3	INIT:RING 3	INIT:CNI,LVL3	INIT:STP:LEVEL=3
4	4	INIT:RING 4	INIT:RING 4	INIT:CNI,LVL4	INIT:STP:LEVEL=4

If IMS loses communication with CNI during an IMS initialization, it escalates to a *UNIX* RTR Operating System Level 2 initialization.

NOTE:
In a 5ESS switch, any failed CNI Level 2, 3, or 4 initialization will trigger a *UNIX* RTR Operating System Level 2 or 3 initialization. In a 1A ESS switch, a failed CNI Level 4 initialization will trigger a *UNIX* RTR Operating System Level 2 initialization.

The *UNIX* RTR Operating System initializations invoke various levels of CNI and IMS initializations. Table 4-C represents a cross-reference of manual *UNIX* RTR Operating System initializations and their corresponding CNI and IMS level initializations.

Table 4-C. CNI/IMS Levels for Corresponding RTR Initializations

Poke Command	RTR Level	CNI Level	IMS Level
50	0	none	none
51	1 1*	none 1	1A 1B
52	2	2	3
53	3	3	3
54	4	3†	3
54‡	4	4§	4

* A CNI Level 1 and an IMS Level 1B occur if a critical IMS process is aborted.

† A CNI Level 3 corresponds to 5ESS® switches.

‡ The 5ESS switch application parameters P (Pump ring), 9 (Pump SMs), R (Generic Retrofit), and S (Generic Retrofit) cause a CNI Level 4 initialization on an RTR Level 4.

§ A CNI Level 4 corresponds to 1A ESS™ switch and 4ESS™ switch and the *A-I-Net*® STP.

Interprocess Message Switch Initialization Level

2.05 The Interprocess Message Switch (IMS) provides five levels of initialization: 0, 1A, 1B, 3, and 4. Their actions are summarized in Table 4-D.

Table 4-D. IMS Initialization Actions

IMS Level	Action
0	This level considers nonboot and generally does not involve any process creation.
1A	This level reinitializes the communications between the 3B20D computer processor and the active Ring Peripheral Controller Nodes (RPCNs). It also restarts Direct Memory Access (DMA) for Direct Link Nodes (DLNs).
1B	This level restarts (without repumping) the active RPCNs. It also restarts DMA for DLNs.
3	This level reinitializes the IMS message switch in the 3B20D computer processor.
4	This level completely reinitializes both the IMS message switch and the ring.

A. IMS Level 0

2.06 An IMS Level 0 initialization simply runs IMS audits. If a problem is found, the audit running takes the necessary corrective action. It is important to note that while the audits are running, access to the IMS message switch is maintained.

2.07 Stimuli causing a Level 0 initialization include: (1) IMS internally requesting a Level 0 initialization and (2) a CNI Level 0 initialization.

2.08 If a Level 0 IMS audit times out waiting to complete, it escalates to an IMS Level 1A initialization.

2.09 The IMS Level 0 and 1A initializations count against an escalation counter. If the number of Level 0 initialization requests in addition to the number of Level 1A initialization requests reaches two within a 1-hour period, a third request for a Level 0 or 1A initialization, occurring within 1 hour of the second request, escalates to an IMS Level 1B initialization.

2.10 If IMS detects discrepancies in the Equipment Configuration Data Base (ECD) during an IMS Level 0 initialization, it aborts the Level 0 initialization and escalates to an IMS Level 3 initialization.

2.11 If IMS loses communication with CNI during an IMS Level 0 initialization, the initialization escalates to a *UNIX* System RTR Level 2 initialization.

B. IMS Level 1A

2.12 An IMS Level 1A initialization initializes communication between the 3B20D computer processor and the Ring Peripheral Controller Nodes (RPCNs), perhaps resulting in some lost messages. It also restarts DLN DMA with the 3B20D computer processor and runs IMS audits. An audit finding a problem takes appropriate corrective action. It is important to note that SS7 calls still complete because the message switch in the 3B20D computer processor is still available.

2.13 Stimuli causing a Level 1A initialization include: (1) IMS internally requesting it, (2) an IMS Level 0 escalated, or (3) an internally invoked CNI Level 1 initialization requested it.

2.14 If a Level 1A IMS audit times out waiting to complete, it escalates to an IMS Level 1B initialization.

2.15 As mentioned earlier, if the number of Level 0 and 1A initialization requests reaches two within a 1-hour period, a third request for a Level 1A, occurring within 1 hour of the second period, escalates to an IMS Level 1B initialization.

2.16 If IMS detects discrepancies in the ECD during a Level 1A initialization, the Level 1A initialization escalates to an IMS Level 3 initialization.

2.17 If IMS loses communication with CNI during an IMS Level 1A initialization, the initialization escalates to a *UNIX* System RTR Level 2 initialization.

C. IMS Level 1B

2.18 An IMS Level 1B initialization stops the IMS message switch and reinitializes it, causing messages to be lost in the process. It initializes communication between the 3B20D computer processor and the DLNs. It also restarts DLN DMA with the 3B20D computer processor. The IMS user processes must close and reopen channels. It is important to note that the Interprocess User Nodes (IUNs) can still communicate with each other during this level of initialization.

2.19 Stimuli of an IMS Level 1B initialization include: (1) IMS internally requesting it, (2) an escalation occurred from an IMS Level 0 or IA initialization, or (3) a manually requested CNI Level 1 initialization.

2.20 If a Level 1B initialization is unsuccessful, it escalates to an IMS Level 3 initialization.

2.21 Like Levels 0 and 1A before it, IMS Level 1B initializations count against an escalation counter. If the number of Level 1B initialization requests reaches two within a 1-hour period, the third request for a Level 1B initialization, occurring within 1 hour of the second request, escalates to an IMS Level 3 initialization.

2.22 If IMS detects discrepancies in the ECD during a Level 1B initialization, the Level 1B initialization escalates to an IMS Level 3 initialization.

2.23 If IMS loses communication with CNI during an IMS Level 1B initialization, the initialization escalates to a *UNIX* System RTR Level 2 initialization.

D. IMS Level 3

2.24 The Level 3 initialization re-creates all the IMS processes in the 3B20D computer processor. In addition, all RPCNs are restored without diagnostics. The previously existing ring communication is maintained if ring communications have not been disrupted. Otherwise, a new ring configuration is determined by ring recovery algorithms. The CNI may call on IMS to download selected ring nodes. Communication among IUNs is maintained except for brief pauses. The DLN DMA within the 3B20D computer processor is also initialized.

2.25 Stimuli for an IMS Level 3 initialization include: (1) the switch application requesting it as a result of a manual request, (2) IMS or CNI having been aborted, (3) a CNI Level 2 initialization request, or (4) a CNI Level 3 initialization request.

2.26 A successful CNI Level 2/IMS Level 3 initialization results in lost call processing. A failed CNI Level 2/IMS Level 3 initialization causes CNI and IMS to abort. The Application Integrity Monitor (AIM) retries another initialization or escalates to a CNI Level 3/IMS Level 3 initialization.

2.27 A failed CNI Level 3/IMS Level 3 initialization causes CNI and IMS to abort. The AIM retries another initialization or escalates to a CNI Level 4/IMS Level 4 initialization.

E. IMS Level 4

2.28 An IMS Level 4 initialization is always done in tandem with a CNI Level 4 initialization. The Level 4 initialization recreates all the IMS processes in the 3B20D computer processor. All ring nodes except the RPCNs are quarantined. Each node is tested to determine if it is able to send messages to the ring. If no faults are found, the ring begins normal operation and token passing. If faults are found, the largest usable part of the ring is initialized and begins token passing. The isolated segment is diagnosed automatically. If too many faults are found, the ring is taken down and communication with the IUNs is not possible.

2.29 If a viable ring is found, program and data files are downloaded to all nodes, including the DLNs. Node restorals on Level 4 are batched so that common programs and data can be broadcast to save time. Any node-dependent data files must be sent separately to each node. Finally, DMA is initialized.

2.30 Stimuli for an IMS Level 4 initialization include: (1) the switch application requesting it as a result of a manual request or (2) IMS having been aborted.

2.31 A failed CNI Level 4/IMS Level 4 initialization causes CNI and IMS to abort. The AIM retries another CNI Level 4/IMS Level 4 initialization. The IMS Level 4 will pump the nodes.

Common Network Interface Initialization Levels

2.32 Common Network Interface (CNI) provides five levels of initialization: 0, 1, 2, 3, and 4. Their actions are summarized in Table 4-E.

Table 4-E. CNI Initialization Actions

CNI Level	Action
0	This level is considered nonboot and generally does not involve any process creation. It causes certain internal CNI and IMS audits to be run.
1	This level is considered nonboot and generally does not involve any process creation. It resets all of the 3B20D computer resident CNI software and reinitializes some of the CNI dynamic data in the ring nodes. If manually invoked, there will be some SS7 downtime.
2	This level reads 3B20D computer resident software in from disk, recreates all CNI processes, and requests an IMS Level 3 initialization.
3	This level reads 3B20D computer resident software and static CNI office dependent data in from disk and recreates all CNI processes.
4	This level is the same as CNI Level 3, in addition to calling an IMS Level 4 initialization, which fully pumps the ring nodes.

A. CNI Level 0

2.33 Having no impact on call processing, a CNI Level 0 initialization invokes CNI kernel process CNIINIT to request CNI and IMS audits be run. The IMS audits are run as a result of CNIINIT requesting an IMS Level 0 initialization.

2.34 Stimuli for a CNI Level 0 initialization include: (1) CNI internally requesting it, (2) the switch SS7 application process CNIINIT requesting it, or (3) a manual craft request.

2.35 If the audits show a large number of noncorrectable errors, CNIINIT escalates the initialization to a CNI Level 1 initialization.

B. CNI Level 1

2.36 A CNI Level 1 initialization resets all of the CNI software resident in the 3B20D computer processor. It reinitializes the CNI dynamic data in the ring nodes. It may invoke an IMS initialization depending on its stimulus. If the stimulus is internal to CNI, no IMS initialization is requested. If the stimulus is a *UNIX* RTR 51 request entered at the Maintenance Control Console, an IMS Level 1A initialization is requested unless a critical IMS process is aborted. In this latter case, an IMS Level 1B initialization is requested.

2.37 If the stimulus is an external request for a CNI Level 1 initialization by the switch's application software, an IMS Level 1B initialization is requested.

2.38 Stimuli for a CNI Level 1 initialization include: (1) CNI internally requesting it, (2) a *UNIX* RTR Level 1 initialization, (3) the switch application software, and (4) an IMS Level 1B initialization resulting in CNIINIT calling for it.

2.39 If CNI fails to complete a Level 1 initialization, it escalates to a CNI Level 2 initialization. In order for this to occur, AIM must recreate CNIINIT.

C. CNI Level 2

2.40 A CNI Level 2 initialization aborts any IMS initialization running and refreshes all 3B20D computer resident CNI software from disk. In addition, all CNI processes are recreated and an IMS Level 3 initialization is requested.

2.41 Stimuli for a CNI Level 2 initialization include: (1) a manual craft request, (2) a result of IMS or CNI having been aborted, and (3) an escalation from a CNI Level 1 initialization failure.

2.42 A failed CNI Level 2/IMS Level 3 initialization causes CNI and IMS to abort. The AIM retries another initialization or escalates to a CNI Level 3/IMS Level 3 initialization.

D. CNI Level 3

2.43 A CNI Level 3 initialization aborts an IMS initialization if one is running. It refreshes all 3B20D computer resident CNI software and also the CNI data base from disk. In addition, all CNI processes are recreated and an IMS Level 3 initialization is requested.

2.44 Stimuli for a CNI Level 3 initialization include: (1) a manual craft request, (2) a result of IMS or CNI having been aborted, and (3) an escalation from a CNI Level 2 initialization failure.

2.45 A failed CNI Level 3/IMS Level 3 initialization causes CNI and IMS to abort. The AIM retries another initialization or escalates to a CNI Level 4/IMS Level 4 initialization.

E. CNI Level 4

2.46 A CNI Level 4 initialization aborts an IMS initialization if one is running. It re-creates all 3B20D computer resident CNI and IMS processes; also the CNI data base from disk. In addition, all CNI processes are recreated, the CNI Protected Address Segment is zeroed out, and an IMS Level 4 initialization is requested.

2.47 Stimuli for a CNI Level 4 initialization include: (1) a manual craft request, (2) a result of IMS having been aborted, or (3) an escalation from a CNI Level 3 initialization.

2.48 A failed CNI Level 4/IMS initialization causes CNI and IMS to abort. The AIM retries another CNI Level 4/IMS Level 4 initialization.

Network Impact

2.49 A series of network events begins when a Lucent Technologies SS7 switch or *A-I-Net* products STP undergoes (for whatever reason) an IMS Level 1B or greater initialization. The chain of events differs depending on whether it is a switch initializing or an *A-I-Net* products STP. The following parts detail both sequences.

A. Lucent Technologies Switch Initialization

2.50 For simplicity, the example network consists of two switches connected by an SS7 trunk and one local *A-I-Net* products STP pair as depicted in Figure 4-6. The Olympus and Sparta offices can be either 1A ESS switches, 4ESS switches, 5ESS switches or any combination thereof. In this scenario, the Olympus office is undergoing a planned CNI Level 4 initialization.

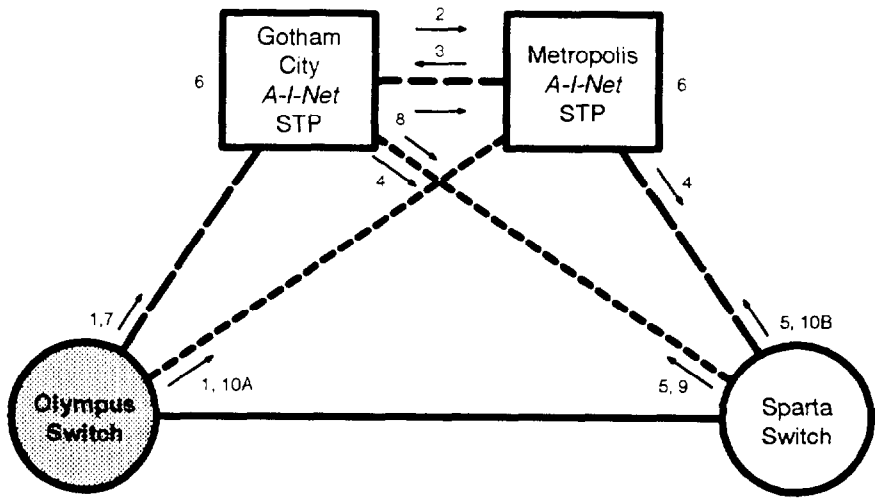


Figure 4-6. Example Network for Switch Initialization

2.51 When the Olympus office initializes the following chain of events occur:

(1) Each Link Node on the CNI ring in the Olympus office sends a Signaling Processor Outage (SIPO) message over its SLK to its corresponding far-end STP (in this case, Gotham City and Metropolis *A-I-Net* products STPs).

(2) When the Gotham City *A-I-Net* products STP receives the SIPO message, a processor outage peg count for the Olympus SLK is incremented in the Network Operations Report and a Transfer Prohibited (TFP) message (concerning the Olympus switch) is sent over the C-links to the Metropolis *A-I-Net* products STP.

(3) When the Metropolis *A-I-Net* products STP receives the SIPO message, it increments the processor outage peg count for the Olympus SLK in the Network Operations Report and sends a TFP message (concerning the Olympus switch) to the Gotham City *A-I-Net* products STP. For illustration purposes, the assumption is made that the bidirectional passage of TFP messages between the *A-I-Net* products STPs occurs simultaneously.

(4) At this point, the Gotham City *A-I-Net* products STP knows its own route to Olympus is unavailable. When it receives a TFP concerning the Olympus switch from the Metropolis *A-I-Net* products STP, it pegs a signaling point isolation counter corresponding to the Olympus SLK in the Network Operations Report and sends a TFP

message (concerning the Olympus switch) to the Sparta switch. Likewise, when the Metropolis *A-I-Net* products STP receives a TFP concerning the Olympus switch from the Gotham City *A-I-Net* products STP, it pegs a signaling point isolation counter for the Olympus SLK in the Network Operations Report and sends a TFP (concerning the Olympus switch) to the Sparta switch.

(5) Receiving the TFP messages concerning the Olympus switch from the Gotham City and Metropolis *A-I-Net* products STPs, the Sparta switch blocks call processing to the Olympus switch and begins sending Signaling Route Set Test (SRST) messages to the *A-I-Net* products STPs. At this point, the Sparta switch considers the Olympus switch isolated and prints the following message on the Maintenance ROP (Table 4-F).

Table 4-F. Switch Output Failure Message

Switch Type	Output Message
1A ESS™	**CCS7 POINT CODE FAILURE dpc**
4ESS™	**REPT: MC3 DOC RECEIVED ON THIS TSG: cin**
5ESS®	**REPT CCS7 POINT CODE FAILURE dpc**

where **dpc** is the Olympus switch's point code and **cin** is the circuit identification number identifying a trunk subgroup connected to the Olympus switch.

(6) Given that the Olympus switch is still initializing, the Gotham City and Metropolis *A-I-Net* products STPs discard the SRST messages because the route status has not changed.

(7) Eventually, the Olympus switch recovers from initializing and prove-in on one SLK completes. For the sake of argument, let us say it is the one connected to the Gotham City *A-I-Net* products STP.

(8) Realizing an SLK to Olympus has completed prove-in, the Gotham City *A-I-Net* products STP broadcasts a Transfer Allowed (TFA) message (concerning the Olympus switch) to the Metropolis *A-I-Net* products STP and the Sparta switch.

(9) On receiving the TFA from the Gotham City *A-I-Net* products STP, the Sparta switch resumes traffic to Olympus and alerts the craft to the fact by the following output message shown in Table 4-G.

Table 4-G. Switch Recovery Output Message

Switch Type	Output Message
1A ESS™	**CCS7 POINT CODE RECOVERED dpc**
4ESS™	**REPT: MC0 DOC RECEIVED ON THIS TSG: cin**
5ESS®	**REPT CCS7 POINT CODE RECOVERED dpc**

where **dpc** is the Olympus switch's point code and **cin** is the circuit identification number identifying a trunk subgroup connected to the Olympus switch.

(10) Two different events can happen at this point.

(a) An SLK between the Olympus office and the Metropolis *A-I-Net* products STP completes prove-in before the Sparta switch sends its next SRST. When this happens, the following events take place:

— The Metropolis *A-I-Net* products STP broadcasts a TFA message (concerning the Olympus switch) to the Gotham City *A-I-Net* products STP and the Sparta switch.

— On receiving the TFA message (concerning the Olympus switch) from the Metropolis *A-I-Net* products STP, the Sparta switch updates its dynamic routing tables and resumes load-sharing Olympus-bound traffic to the Gotham City and Metropolis *A-I-Net* products STPs. At this point, the network is back to normal operation.

(b) The Sparta switch sends an SRST message to the Metropolis *A-I-Net* products STP before an SLK between the Olympus switch and Metropolis *A-I-Net* products STP can prove-in. When this happens, the following events occur:

— The Metropolis *A-I-Net* products STP discards the SRST message from Sparta.

— The Metropolis *A-I-Net* products STP sends a Transfer Restricted (TFR) message (concerning the Olympus switch) to the Sparta switch.

— The Sparta switch continues to send SRST messages to the Metropolis *A-I-Net* products STP until it receives a TFA concerning the Olympus switch from the Metropolis *A-I-Net* products STP.

— Eventually, an SLK between the Olympus switch and the Metropolis *A-I-Net* products STP completes prove-in.

— The Metropolis *A-I-Net* products STP broadcasts a TFA message (concerning the Olympus switch) to the Gotham City *A-I-Net* products STP and the Sparta switch.

— On receiving the TFA message from the Metropolis *A-I-Net* products STP, the Sparta switch updates its dynamic routing tables and resumes traffic to the Olympus switch. At this point, the network is back to normal operation.

NOTE:
While the Olympus switch is initializing, all interoffice SS7 calls are inhibited. Only when one of the Olympus switch's SLKs completes prove-in can normal SS7 call processing resume.

B. *A-I-Net* Products STP Initialization

2.52 The example network (Figure 4-7) is used to show the chain of network events resulting from an *A-I-Net* products STP initialization. Again, the Olympus and Sparta offices can be either 1A ESS switches, 4ESS switches, 5ESS switches or any combination thereof. In this scenario, the Gotham City *A-I-Net* products STP is undergoing a planned CNI Level 4 initialization.

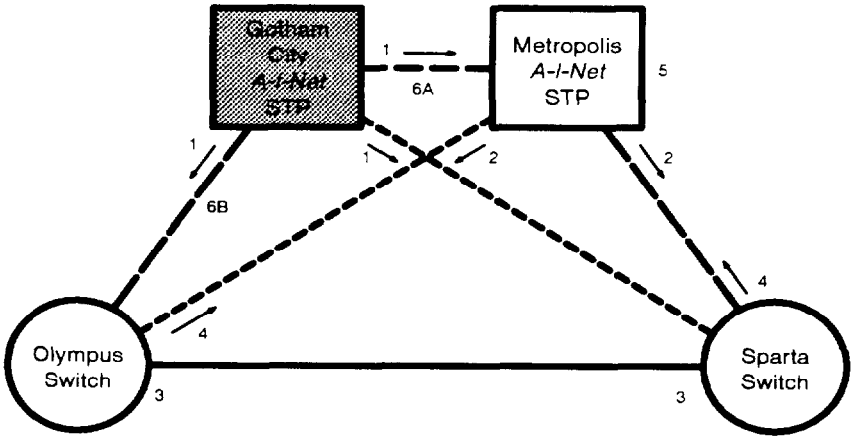


Figure 4-7. Example Network for *A-I-Net* Products STP Initialization

2.53 When the Gotham City *A-I-Net* products STP initializes, the following chain of events occurs:

(1) Each link node on the CNI ring in the Gotham City *A-I-Net* products STP sends a SIPO message over its SLK to its corresponding local signaling point (that is, the Metropolis *A-I-Net* products STP and the Olympus and Sparta switches).

(2) When the Metropolis *A-I-Net* products STP receives the SIPO message, it reports that contact is lost with the Gotham City *A-I-Net* products STP processor (that is **REPT CNCE** critical events C7POR) accompanied by a C7LSF and a C7SPI and responds with a TFP message (concerning the Gotham City *A-I-Net* products STP) to Olympus and Sparta offices.

(3) When the Olympus and Sparta switches receive the TFP message, the craft is notified that communication is lost with the Gotham City *A-I-Net* products STP processor; that is, **REPT CNCE** critical events:

— C7POR—due to SIPO received from Gotham City *A-I-Net* products STP.

— C7LSF—for the linkset to Gotham City.

— C7SPI—concerning Gotham City STP point code due to the prior C7LSF and the received TFP.

(4) Load sharing between the *A-I-Net* products STPs is stopped with all signaling now being routed through the Metropolis *A-I-Net* products STP.

(5) Realizing the SLKs to the Gotham City *A-I-Net* products STP are unavailable for normal SS7 call processing, the Olympus and Sparta offices route all signaling through the Metropolis *A-I-Net* products STP and begin sending Signaling Route Set Test (SRST) messages to the Metropolis *A-I-Net* products STP.

(6) Given that the Gotham City *A-I-Net* products STP is still initializing, the Metropolis *A-I-Net* products STP discards the SRST message because the route status has not changed.

(7) At this point, one of two events usually happens.

(a) An SLK (C-link) between the Gotham City and Metropolis *A-I-Net* products STPs stops receiving SIPO and completes prove-in. When this happens, the following events occur:

- The Metropolis *A-I-Net* products STP broadcasts a TFA message (concerning the Gotham City *A-I-Net* products STP) to the Olympus and Sparta offices and reports **REPT CNCE** critical events C7SPIE, C7LSFE, and C7PORE concerning the Gotham City *A-I-Net* products STP.
- On reception of the TFA (concerning the Gotham City *A-I-Net* products STP) from the Metropolis *A-I-Net* products STP, the Olympus and Sparta switches can communicate with the Gotham City *A-I-Net* products STP via the Gotham and Metropolis *A-I-Net* products STP C-links. Craft personnel are notified that communication is available by *REPT CNCE* critical events **C7SPIE**. Traffic destined for the Gotham City *A-I-Net* products STP is routed to the Metropolis *A-I-Net* products STP and over the C-links.
- Eventually, an SLK (A-link) between the Gotham *A-I-Net* products STP and the Sparta switch stops receiving SIPO and completes prove-in. This is evidenced by **REPT CNCE** critical events C7LSFE and C7PORE. The Sparta switch resumes load-sharing traffic between the Gotham City and Metropolis *A-I-Net* products STPs.
- Likewise, an SLK (A-link) between the Gotham *A-I-Net* products STP and the Olympus switch stops receiving SIPO and completes prove-in. This is also evidenced by **REPT CNCE** critical events C7LSFE and C7PORE. The Olympus switch resumes load-sharing traffic between its local *A-I-Net* products STPs.

(b) An SLK (A-link) between the Gotham City *A-I-Net* products STP and either the Olympus or Sparta switch completes prove-in. For the sake of illustration, let us say the Olympus SLK completes prove-in. When this happens, the following events occur:

- **REPT CNCE** critical events C7FSPIE, C7LSFE, and C7PORE are reported to the Olympus craft. The Olympus switch resumes load-sharing traffic between the Gotham and Metropolis *A-I-Net* products STPs.
- Eventually, an SLK (C-link) between the Gotham City and Metropolis *A-I-Net* products STPs completes prove-in. When this happens, the Metropolis *A-I-Net* products STP broadcasts a TFA message (concerning the Gotham City *A-I-Net* products STP) to the Olympus and Sparta office. and reports the **REPT CNCE** critical event C7SPIE concerning the Gotham City *A-I-Net* products STP. The Sparta switch receiving TFA will report the REPT CNCE critical event C7SPIE concerning Gotham City.
- Eventually, an SLK (A-link) between the Gotham *A-I-Net* products STP and the Sparta switch completes prove-in. This is evidenced by **REPT CNCE** critical events C7LSFE and C7PORE. The Sparta switch resumes load-sharing traffic between both *A-I-Net* products STPs.

NOTE:
Due to the mated architecture in this network, no interoffice SS7 calls are lost during a single *A-I-Net* products STP initialization. But, if all SLKs between the Metropolis *A-I-Net* products STP and the Olympus office fail while the Gotham City *A-I-Net* products STP is initializing, the Olympus office is isolated and SS7 traffic stops until SLK connectivity is established with either *A-I-Net* products STP.

CAUTION:
If the Olympus (or Sparta) switch defines individual Global Title A-I-Net products STP point codes, Global Title Translation (GTT) messages to the initializing Gotham City *A-I-Net* products STP may be returned to the switch indicating the point code is inaccessible. When the TFP from Metropolis is processed, all GTTs to Gotham City stop. However, if a capability code (or alias point code) is defined, the GTT messages are translated by the Metropolis *A-I-Net* products STP and sent along on the determined path.

3. CNI Hardware Trouble

Ring Maintenance States

3.01 The CNI ring has certain IMS maintenance states that are maintained. It is important to know the maintenance states for the ring hardware when troubleshooting a hardware problem.

3.02 The ring maintenance state defines the overall operational state of the ring. It consists of the following:

(1) **Ring Normal**—This is a normal 2-ring configuration. There are no isolated nodes in the ring.

(2) **Ring Isolated**—The ring contains an isolated segment. The beginning of the isolation (BISO) and the end of isolation (EISO) nodes are active.

(3) **Ring Restoring**—The ring contains an isolated segment and the restoral activity is in progress on newly assigned BISO and/or EISO nodes. This is a transient state that can last several minutes.

(4) **Ring Down**—The ring is totally unusable from the 3B20D computer processor. However, the IUNs (IMS User Nodes) may be able to communicate among themselves.

(5) **Ring Configuring-No BISO/EISO**—This is the same as the Ring Configuring state with the ring in a normal 2-ring configuration without BISO and EISO nodes. It is a transient state.

(6) **Ring Configuring-Isolated**—This is the same as the Ring Configuring state with the ring containing an isolated segment. It is a transient state.

3.03 The IMS node major state shows the overall status of a node during normal system operation. The major state is the same as the ECD data. The major states are as follows:

ACT (Active)	The node is active and performing on-line functions.
STBY (Standby)	The node is an RPCN or DLN that is operating, but the ring configuration is not completed, or the ring is down.
INIT (Initializing)	The node is initializing. This is a transient state used to restart nodes on the ring.
OOS (Out-Of-Service)	The node is OOS and unavailable for normal use, but can be used for maintenance and diagnostic purposes.

GROW (Grow) — The node is physically being added or removed from the ring. The node must always be configured within an isolated segment of the ring. This state is entered only by changing the ECD.

UNEQ (Unequipped) — The node is unequipped, but an ECD record can exist for this node.

3.04 The **OP:RING** input message (**DETD** keyword) gives the node major state in a single letter format. While uppercase letters indicate the active portion of the ring, lowercase letters indicate the isolated portion of the ring, as shown in Table 4-H.

Table 4-H. Meanings of OP:RING Status Indicators

Status	Active Segment	Isolated Segment or Ring Down
Active	A	–
Standby	S	s
Unavailable	U	u
Out-of-Service	O	i
Initializing	B	b
Unequipped	•	•

3.05 The node minor state for ring position indicates the position of each node relative to the current configuration of the ring. The state values of ring position 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) **BISO** (Begin Isolated Segment)—The node is included in the active ring and forms the beginning of the isolated segment.

(3) **EISO** (End Isolated Segment)—The node is included in the active ring and forms the end of the isolated segment.

(4) **ISO** (Isolated)—The node is contained in the isolated segment.

3.06 The node minor state for node processor (NP) hardware indicates the maintenance state of the hardware. The state values include:

(1) **USBL** (Usable)—The node processor is usable.

(2) **FLTY** (Faulty)—The node processor is known to be faulty or is suspected of being faulty.

(3) **UNTSTD** (Untested)—The condition of the node processor is unknown and is presumed faulty.

3.07 The node minor state for Ring Interface (RI) hardware indicates whether a node can be included in the active ring. The RI hardware states include:

(1) **USBL** (Usable)—The RI hardware is usable.

(2) **QUSBL** (Quarantine Usable)—The RI hardware is partially usable. The node can be included in the active ring, but the node must be in the quarantine (that is, OOS) state.

(3) **FLTY** (Faulty)—The RI hardware is faulty and the node must be isolated.

(4) **UNTSTD** (Untested)—The condition of the RI hardware is unknown and is treated as though it was isolated.

3.08 The node minor state for maintenance mode indicates whether automatic restoral of the node is attempted by Automatic Ring Recovery (ARR). The state values include:

(1) **AUTO** (Automatic)—The node is under the automatic control of ARR.

(2) **MAN** (Manual)—The node is under manual control and only manual user action can restore the node to service.

3.09 The node major and minor states can be viewed on the following display pages as shown in Tables 4-I. Valid ring maintenance state, node major state, and ring position combinations are shown in Tables 4-J, 4-K, and 4-L.

Table 4-I. Switch View Pages for Major and Minor States

1A ESS™ Switch	4ESS™ Switch	5ESS® Switch	*A-I-Net*® STP
1106	1106	1520	1141, 1142

Table 4-J. Valid Ring Maintenance State Combinations

Ring Maintenance State	Ring Major State	Ring Position
RING NORMAL	ACT OOS	NORM NORM
RING ISOLATED	ACT OOS ACT ACT OOS	NORM NORM BISO EISO ISO
RING DOWN	STBY (RPCNs) OOS	ISO ISO

Table 4-K. Valid Node Major State and Ring Position Combinations

Node Major State	Node Minor State Ring Position	Processing Messages in Node	Passing Messages Around Ring
ACT	NORM	YES	YES
ACT	BISO	YES	YES
ACT	EISO	YES	YES
OOS	NORM	NO	YES
OOS	ISO	NO	NO
OOS	BISO*	NO	YES
OOS	EISO*	NO	YES

* BISO and EISO nodes with OOS major state are used only when necessary.

3.10 The node major state and ring position are related to the NP and RI hardware states as shown in Table 4-L.

Table 4-L. Node Major State and Ring Position

Major State	Node Minor State		
	Ring Position	NP Hardware	RI Hardware
ACT	NORM	USBL	USBL
ACT	BISO	USBL	USBL
ACT	EISO	USBL	USBL
OOS	NORM	FLTY, UNTSTD	USBL
OOS	NORM	USBL	QUSBL
OOS	NORM	FLTY, UNTSTD	QUSBL
OOS	ISO	ANY	FLTY, UNTSTD
INIT	NORM	USBL	USBL
INIT	BISO	USBL	USBL
INIT	EISO	USBL	USBL

Fault Detection

3.11 The CNI/IMS ring does not rely on routine diagnostics to detect hardware faults. In its place are a number of fault detection and recovery mechanisms built into the design.

3.12 Ring faults are detected in a number of ways. The primary means for detecting a hardware problem is through a strategy whereby a node "blocks" message transport if it detects errors. This condition is known as ring blockage. Blockage occurs when a node detects, for example, bad parity on a message passed to it on ring 0 by an upstream node. It reacts by not returning the Data Taken signal. This signal is used to notify the upstream node that it received the data. The upstream node blockage timer expires waiting for the Data Taken signal, causing it to initiate blockage recovery. Blockage recovery isolates the downstream node attributed with the error. The upstream node notifies the 3B20D computer processor of blockage detected via ring 1.

3.13 Ring transport errors, reported on the Receive-Only Printer (ROP) by means of the **REPT RING TRANSPORT ERR** output message, are usually indicative of a problem in an associated node's Ring Access Circuit (RAC) circuitry and may cause a node to intentionally force blockage, leading to isolation of the affected portion(s) of the ring. The type of problems include:

(a) **BLOCKAGE**—A node's blockage timer expires while waiting for a ring transfer to occur (that is, no Data Taken signal returned).

(b) **RAC PARITY/FORMAT ERROR**—Two cases: (1) a ring data byte with bad parity is offered to the node and node recovery action cannot clear the error, and (2) an "orphan byte" is offered to the node. An orphan byte condition occurs when the node expects a control byte, but the byte offered is not a control byte.

(c) **TRANSIENT RAC ERROR**—A ring data byte with bad parity is offered to the node and node recovery clears the error (that is, the message is resampled).

(d) **INTERFRAME BUFFER PARITY ERROR**—The upstream Interframe Buffer (IFB) detects a ring parity error. This error can result in forced blockage.

(e) **RAC OUTPUT PARITY ERROR**—Data with bad parity is read from the ring during ring blockage recovery.

(f) **WRITE FORMAT ERROR**—Some error occurs while a node is attempting to write a message to the ring. This error can result in forced blockage.

(g) **INPUT FORMAT ERROR**—A partial message, shorter than an IMS header, is read into NP memory.

(h) **READ INHIBIT ERROR**—Blockage occurs during a read or while propagating a message and no data is read into NP memory.

(i) **SOURCE MATCH**—A ring message returns to the sending node because the destination node did not remove the message from the ring.

(j) **GENERAL RAC ERROR**—A "catchall" error type used to report an unexpected node hardware or software condition.

(k) **SOFT RAC PARITY ERROR**—A threshold for parity errors is exceeded.

(l) **UNEXPLAINED LOSS OF TOKEN**—The RPCNs report a loss of the ring token to the 3B20D computer processor and no node has reported another ring transport error type to identify the location of the ring problem. A ring configuration is requested to test the continuity of the various ring segments and reinsert the token in the newly selected active ring.

(m) **READ FORMAT ERROR**—The node receives a message shorter than the message header indicates it should be, but at least as long as an IMS message header.

(n) **READ TOO SHORT ERROR**—A node reads a message that is shorter than an IMS header (8 bytes). The partial message header is discarded.

(o) **DEQUEUED TOKEN**—A ring node reports this error when it finds that it has read the token message from the ring. This error is intended to detect failures that cause a node to inadvertently read data from the ring.

3.14 There is a set of ring transport errors that indicate either an internal node problem or a problem detected by another node that does not involve the RAC circuitry. These errors cause the defective node to be removed from service without reconfiguring the ring (the node is shown as quarantined on OP:RING). They include:

(a) **SRC MATCH**—This is the same as the SOURCE MATCH error, except the detection is made by the Node Audit (NAUD) operation.

(b) **NAUD FAILURE**—The node audit operation fails a communication test with a node.

(c) **RING WRITE FAILURE**—An RPCN reports that it failed in writing a message to the active ring.

(d) **RING READ FAILURE**—An RPCN reports that it failed in reading a message from the active ring.

(e) **RPCN PANIC**—This is a failure condition in RPCN software.

(f) **UNXPCTD SET QUAR**—The 3B20D computer receives an unprovoked confirmation from an RPCN that it has been directed to quarantine itself.

(g) **RAC CONTROL FAILURE**—During ring maintenance activity, the ability of the 3B20D computer to control an RPCN's RAC fails.

(h) **MSG RELAY FAILURE**—This is similar to the RING WRITE FAILURE. An RPCN fails to relay a message from the 3B20D computer to the ring during ring maintenance activity.

(i) **RING INTERFACE FAILURE**—During a boot, ring maintenance activity finds an RPCN's ring interface to be faulty.

(j) **PIO FAILURE**—A Programmed Input/Output (PIO) operation at an RPCN from the 3B20D computer fails.

(k) **RPCN STATE CHANGE FAILURE**—The RPCN fails to confirm that it has followed a 3B20D computer directive to change to a particular software state during ring maintenance activity.

(l) **RPC ISOLATION**—Multiple ring faults previously reported elsewhere on the ring cause the RPCN to be conditionally isolated. This condition is reported as a ring transport error but is actually a status message. The isolation is conditional because the RPCN may or may not be an innocent victim. It is presumed that the RPCN itself is not faulty.

(m) **UNXPCTD STATE CHNG MSG**—This is similar to the RPCN STATE CHANGE FAILURE. Without having been sent a 3B20D computer directive, an RPCN reports that it has changed to a particular software state.

Node Audit

3.15 The Node Audit (NAUD) replaces the Neighbor Node Audit (NNAUD) in the following software releases as shown in Table 4-M.

Table 4-M. Node Audit Generic Software Releases

1A ESS™ Switch APS	4ESS™ Switch APS	5ESS® Switch	*A-I-Net*® STP
1AP3D or later	4AP9 or later	5E7 or later	Release 0 or later

3.16 The NAUD audit deploys an auditing strategy different from that used by the NNAUD. Instead of a node sending its neighbors a test message periodically, the 3B20D computer processor tests each active node on the ring one at a time. The processor first selects a "control" RPCN through which to send messages and then selects an active node on the ring to audit.

⇒ NOTE:
Each time a NAUD request is sent, the control RPCN that is chosen will be rotated among the active RPCNs. The chosen RPCN will be used for all messages pertaining to the audit cycle. When the next node is audited, the next active RPCN will be used. This will test the ring path through all RPCNs.

3.17 The 3B20D computer processor passes a NAUD request message to the selected node followed by a ring "chaser" message that will traverse the entire ring and return to the 3B20D computer processor. The ring chaser message will verify the operation of the Direct Memory Access (DMA) channel to an RPCN, the RPCN itself, and the ring.

3.18 In the normal case, the node receives the NAUD request message and replies back to the 3B20D computer processor through the control RPCN with a NAUD response message. The 3B20D computer processor will receive the NAUD response and ring chaser messages and select the next node to audit.

3.19 Two failures may result from each initial NAUD attempt: (1) the node itself fails to send a NAUD response message to the 3B20D computer processor or (2) the ring chaser message fails to return. Both of these scenarios are discussed below:

(a) Node NAUD Response Failure

(b) Ring Chaser Message Failure.

A. Node NAUD Response Failure

3.20 If the 3B20D computer processor fails to receive the NAUD response message, a new control RPCN (if available) will be selected and a second NAUD request will be sent to the selected node along with another ring chaser message.

⇒ NOTE:
If a new control RPCN is not available, the existing control RPCN will be used on this second attempt.

3.21 If a NAUD response is not detected on this second try, the node is faulted. The defective node will be removed from service without reconfiguring the ring. Although a minor alarm is sounded when this occurs, normally no user interaction is required. A **REPT RING TRANSPORT ERR** output message will be reported. An example message is provided below.

REPT RING TRANSPORT ERR
RMV LN00 3 RQSTD: NAUD FAILURE

3.22 The Automatic Ring Recovery (ARR) process (described later in this chapter) will run diagnostics on the node to determine the exact nature of the problem. The ARR process will unconditionally restore the node once the isolation has cleared. In the event that ARR cannot recover the node, manual intervention will be needed.

B. Ring Chaser Message Failure

3.23 If the 3B20D computer processor fails to receive the ring chaser message, another active RPCN is selected. If no other RPCN is available, the failure cannot be differentiated between the RPCN and the ring. In this case, a **REPT RING TRANSPORT ERR** output message is reported and a Level 3 Error Analysis and

Recovery (EAR) (discussed later in this chapter) is invoked to attempt to isolate a ring problem if one exists. An example of the output message is given below.

REPT RING TRANSPORT ERR
NAUD DETECTS RPCN32 0 PROBLEM OR RING MESSAGE LOSS

3.24 If a second active RPCN is available, a ring chaser message is sent through it. If this chaser message is received by the 3B20D computer processor, the first control RPCN is removed for a diagnostic restore. A **REPT RING TRANSPORT ERR** output message will be reported. An example of the output message is given below.

REPT RING TRANSPORT ERR
RMV RPCN32 0 RQSTD: NAUD CONTROL RPC FAILURE RPTD BY RPCN00 0

3.25 If the message is not received, a failure between two RPCNs is assumed to be a ring problem. The following **REPT RING TRANSPORT ERR** output message is reported and a Level 3 EAR is invoked.

REPT RING TRANSPORT ERR
NAUD DETECTS RING MESSAGE LOSS

For an explanation of these examples, refer to appropriate switch or *A-I-Net* products STP output manual.

Fault Recovery and Troubleshooting

3.26 There are two software mechanisms which work together to provide automatic ring recovery when faults are detected: the Error Analysis Recovery (EAR) and Automatic Ring Recovery (ARR) systems.

3.27 The EAR provides rapid, automatic recovery from faults it detects. It has centralized control in the 3B20D computer processor and provides for distributed error detection and partial recovery in the ring nodes. The EAR uses quarantine (that is, OOS) and isolation to remove faulty hardware.

3.28 The ARR is used for deferrable ring fault recovery. This includes automatic diagnostics and restoral of nodes that are removed and/or isolated by EAR and application-requested automatic removal.

3.29 Another capability called Application Critical Node Restore (ACNR) enables the application to request a restore of a ring node independent of ARR's normal action. It provides the ability to restore DLNs or LNs it considers critical to its operation in a more timely manner. These restore requests, however, are subject to ARR's rules and regulations.

A. Error Analysis and Recovery

3.30 The EAR is responsible for determining the probable cause of a fault(s), the location of the fault, and then, if necessary, requests a ring configuration to remove the faulty equipment from the active ring. Traffic is routed around the affected equipment, allowing ARR attempts to restore the faulty equipment to the ring. The EAR employs six levels of ring recovery. Table 4-N displays these levels.

Table 4-N. Levels of Error Analysis and Recovery

Level	Action
0	An attempt is made to establish the original configuration. This is the first level if the alternative is large isolation.
1	An attempt is made to establish a viable configuration based on detected errors. This is the most common level of recovery.
2	There are two cases: (1) This level expands the isolated segment by one node in each direction and retries if a Level 1 failed to establish a viable ring configuration. (2) This level expands the isolated segment to include any additional faulty nodes if the ring fails within 5 seconds of a successful configuration.
3	Communication continuity on the ring between each pair of adjacent RPCNs is determined. From this, EAR pieces together the largest possible ring segment and performs a binary search for fault(s) in the remaining ring section. The results from this define how the ring configuration is attempted.
4	An attempt is made to establish a minimal ring configuration and expand it iteratively to encompass as much of the ring as possible.
5	This level is similar to Level 4, but a longer soak period for added nodes is used.

3.31 When EAR detects problems in the ring, it changes maintenance states to communicate its actions and its knowledge. Thus node problems can be mapped directly to IMS maintenance states and EAR actions as shown in Table 4-O.

Table 4-O. Node Problems Mapped to MTCE States and EAR Actions

Node States	Maintenance States					EAR Response
	Node State	Ring Position	RI State	NP State	Maint. Mode	
None	ACT	NORM, BISO, or EISO	USBL	USBL	AUTO	None
Local restart of a DLN or RPCN	INIT	NORM, BISO, or EISO	USBL	USBL	AUTO	None
Faulty NP or auxiliary component	OOS	NORM, BISO, or EISO	USBL	FLTY	AUTO	Quarantine the node
Application request to test the user interface	OOS	NORM, BISO, or EISO	USBL	USBL	AUTO	Quarantine the node
Faulty RI hardware (but no interference with propagating messages on ring)	OOS	NORM	QUSBL	USBL	AUTO	Quarantine the node
Faulty RI hardware	OOS	ISOL	FLTY	USBL	AUTO	Isolate the node
Innocent Victim	OOS	ISOL	USBL	USBL	AUTO	Isolate the node
Faulty NP or auxiliary component and faulty RI	OOS	ISOL	FLTY	FLTY	AUTO	Isolate the node
Needed to form an isolated segment	ACT	BISO	USBL	USBL	AUTO	Configure as BISO node
Needed to form an isolated segment	ACT	EISO	USBL	USBL	AUTO	Configure as EISO node
Untested NP	OOS	NORM	USBL	UNTSTD	AUTO	Quarantine the node

B. Automatic Ring Recovery

3.32 Automatic Ring Recovery (ARR) is responsible for automatically restoring faulty nodes, innocent victim nodes, and nodes marked OOS that are found to be in appropriate maintenance states. The ARR's action is dependent on the various combinations of minor and ring maintenance states associated with the OOS major state as shown in Table 4-P.

Table 4-P. ARR Responses to Ring Maintenance States

Isolated	RI State	NP State	NM State	ARR Action
YES	FLTY, QUSBL	ANY	AUTO	COND RST (*)
YES	UNTSTD	ANY	AUTO	COND RST (*)
YES	USBL	ANY	AUTO	NONE
YES	ANY	ANY	MAN	NONE
NO	USBL	USBL	AUTO	UCL RST
NO	USBL	UNTSTD, FLTY	AUTO	COND RST
NO	USBL	ANY	MAN	NONE
NO	QUSBL	ANY	AUTO	COND RST
NO	QUSBL	ANY	MAN	NONE
NO	UNTSTD, FLTY	ANY	ANY	ERRLOG,RI=QUSBL, reprocess

* A conditional restore is performed unless the node is surrounded by other RI=FLTY or RI=UNTSTD nodes. If this is the case, no action is taken until node is reachable from at least one direction. The conditional restore requests inclusion in the ring if RI tests pass. Usable hardware states are transient during the conditional restore.

3.33 The ARR responds to any node in the OOS major state that has not been placed in OOS for manual reasons. A source of automatic removal other than IMS fault recovery is a CNI request via a software interface. One such case is an SLK prove-in failure. If an SLK fails prove-in, it removes the LN from service. The ARR then attempts to recover LN.

3.34 The ARR normally attempts to restore any node once. If diagnostics fail, the faulty equipment is marked faulty, and manual action is required. If diagnostics are started and subsequently abort with no test failures indicated, ARR attempts to restore a node a maximum of three times before any manual actions are requested. The actions previously mentioned are summarized in Table 4-Q.

NOTE:
The Application Critical Node Restoral (ACNR) capability, if active, will override all ARR actions shown in the following table.

Table 4-Q. ARR Responses to Node Failures/Restorals

Node State	Ring Pos.	RI State	NP State	Fail/Rst Condition	ARR Actions	
					First	Second
ACT	NORM	USBL	USBL	n/a	None	
OOS	NORM	USBL	FLTY	1st or 2nd	pump and return	
				3rd	isolate and	pass - pump and return to service
				4th failure/hr.	manual maintenance	
OOS	NORM	USBL	UNTSTD	n/a	pump and return to service	
OOS	NORM	QUSBL	FLTY	any failure	isolate and diagnose	pass - pump and return to service fail - manual maintenance
OOS	NORM	USBL	FLTY	ext. node failure	isolate and diagnose	pass - pump and return to service fail - manual maintenance
OOS	ISOL	FLTY	USBL	up to 3rd failure/hr.	isolate and diagnose	pass - pump and return to service fail - manual maintenance
				4th failure/hr.	manual maintenance	
OOS	ISOL	FLTY	FLTY	up to 3rd failure/hr.	isolate and diagnose	pass - pump and return to service fail - manual maintenance
				4th failure/hr.	manual maintenance	
OOS	ISOL	USBL	FLTY	any failure	quarantine	manual maintenance
OOS	ISOL	USBL	USBL	isolation ends	pump and return to service	
ACT	BISO	USBL	USBL	isolation ends	set BISO to NORM	
ACT	EISO	USBL	USBL	isolation ends	set EISO to NORM	

3.35 If equipment is automatically removed from service for fault reasons, manual actions SHOULD BE AVOIDED until ARR has attempted to restore the equipment, and marks it for manual actions. If manual actions are desired, then to avoid conflicting with the ARR, ARR may be inhibited using the **INH:DMQ** input message. To determine which nodes are marked for automatic restoral and/or queued for automatic restoral, enter the **OP:DMQ** input message.

NOTE:
Inhibiting ARR does not inhibit unconditional restorals (that is, they are still active). It only blocks conditional restorals.

3.36 The OOS nodes eligible for automatic restorals are determined by priority. The priority listing and order of node restoral is as follows:

(1) Nodes serving as BISO/EISO.

(2) Nodes with faulty ring interfaces. This also includes nodes within an isolated segment and with an RI state of UNTSTD.

(3) The RPCNs eligible for unconditional restoral.

(4) The User Critical Node high priority.

(5) The RPCNs eligible for conditional restoral.

(6) The User Critical Node low priority.

(7) The LNs eligible for unconditional restoral.

(8) The LNs eligible for conditional restoral.

3.37 When diagnosing and attempting to restore nodes within an isolated ring segment, ARR attempts to restore the end nodes of the isolated segment. These end nodes are those adjacent to either the BISO or EISO nodes. The inner nodes of the isolated segment are called innocent victim nodes when they are not inherently faulty.

3.38 Table 4-R shows the correlation between an ARR action/result and its corresponding output message.

Table 4-R. Output Messages Due to ARR Actions/Results

ARR Action or Result	Output Message
Request to quarantine an RPCN	RMV RPCN...
Request to quarantine an LN	RMV LN...
Request to quarantine a DLN	RMV LN... (4ESS™ and 5ESS® Switches) RMV DLN... (1A ESS™ Switch)
Request to diagnose an RPCN	DGN RPCN...
Request to diagnose an LN	DGN LN...
Request to diagnose a DLN	DGN LN... (4ESS and 5ESS Switches) DGN DLN... (1A ESS Switch)
Request to diagnose and restore an RPCN to service	RST RPCN...
Request to diagnose and restore an LN to service	RST LN...
Request to diagnose and restore a DLN to service	RST LN... (4ESS and 5ESS Switches) RSI DLN... (1A ESS Switch)
Abort a diagnostics request due to an error	DGN AUDIT RING...
Report outcome of a request to reconfigure the ring	REPT RING CFR
Abort an IUN pump	REPT IUN PUMP...
Report a failure of an IUN restore	REPT IUN RST...
Report a failure of an RPCN initialization during a restore or restart	REPT RPC INIT...
Start an ARR recovery attempt	REPT ARR AUTORST a b FOR c STARTED
Report success of ARR recovery attempt	REPT ARR AUTORST a b FOR c SUCCEEDED
Report failure of a diagnostic phase	REPT ARR AUTORST a b FOR c FAILED
Abort a diagnostic request	REPT ARR AUTORST a b FOR c ABORTED
Report violation of 4th-time rule	REPT ARR AUTORST RECOVERY THRESHOLD EXCEEDED FOR c
Time out a restoral request	REPT ARR AUTORST TIMEOUT AWAITING MIRA FOR c
Inhibit a restoral request	REPT ARR AUTORST a b FOR c STOPPED <INHIBITED>

Useful Input Controls

3.39 Some useful ARR input controls are provided to manually take control over ARR recovery actions. Table 4-S summarizes these controls.

Table 4-S. ARR Input Controls

Action	Input Request	
Inhibits ARR conditional restorals; (unconditional ARR restorals are still active).	INH:DMQ;SRC ARR INH:DMQ:SRC=ARR	(1A ESS™ and 4ESS™ Switches) (5ESS® Switch, *A-I-Net*® STP)
Displays the active and queued restoral requests.	OP:DMQ	
Stops active and queued conditional requests.	STOP:DMQ	
Remove the RPCN from service.	RMV:RPCNxx y RMV:RPCNxx=y	(1A ESS and 4ESS Switches) (5ESS® Switch, *A-I-Net*® STP)
Remove the LN from service.	RMV:LNxx y RMV:LNxx=y	(1A ESS and 4ESS Switches) (5ESS Switch, *A-I-Net* STP)
Remove the DLN from service.	RMV:DLNxx y RMV:LNxx y RMV:LNxx=y	(1A ESS Switch) (4ESS Switch) (5ESS Switch)
Remove the RPCN from service (if not already) and run diagnostic tests.	DGN:RPCNxx y DGN:RPCNxx=y	(1A ESS and 4ESS Switches) (5ESS Switch, *A-I-Net* STP)
Remove the LN from service (if not already) and run diagnostic tests.	DGN:LNxx y DGN:LNxx=y	(1A ESS and 4ESS Switches) (5ESS Switch, *A-I-Net* Products STP)
Remove the DLN from service (if not already) and run diagnostic tests.	DGN:DLNxx y DGN:LNxx y DGN:LNxx=y	(1A ESS Switch) (4ESS Switch) (5ESS Switch)
Force remove the LN from service, regardless of the **state** of link, mate, or other nodes.	FRMV:LNxx Y FRMV:LNxx Y	(1A ESS and 4ESS Switches) (5ESS Switches)
Force remove the DLN from service, regardless of the **state** of the mate, or other nodes.	FRMV:DLNxx Y FRMV:LNxx Y FRMV:LNxx=Y	(1A ESS Switch) (4ESS Switch) (5ESS Switches)
Restore the RPCN to service conditionally or unconditionally as desired.	RST:RPCNxx y RST:RPCNxx=y	(1A ESS and 4ESS Switches) (5ESS Switch, *A-I-Net* products STP)
Restore the LN to service conditionally or unconditionally as desired.	RST:LNxx y RST:LNxx=y	(1A ESS and 4ESS Switches) (5ESS Switch, *A-I-Net* Products STP)
Restore the DLN to service conditionally or unconditionally as desired.	RST:DLNxx y RST:LNxx y RST:LNxx=y	(1A ESS Switch) (4ESS Switch) (5ESS Switch)
Force removal from service and restart the LN regardless of the **state** of and *A-I-Net* Products STP) other nodes. The LN is initialized without pumping.	INIT:LNxxY INIT:LNxx Y	(1A ESS and 4ESS Switches) (5ESS Switch
Force removal from service and restart for the specified DLN, regardless of the **state** of other nodes. The DLN is initialized without pumping. A successful restart returns the DLN to service.	INIT:DLNxx Y INIT:LNxx Y INIT:LNxx = Y	(1A ESS Switch) (4ESS Switch) (5ESS Switch)

Manual Diagnostics and Troubleshooting

3.40 Diagnostics of RPCNs, LNs, and DLNs may be performed manually. When the system detects a fault, however, diagnostics are performed automatically by ARR. If manual diagnostics are desired on a node that is automatically removed, the node's minor state for maintenance should be checked to determine if it is under manual control. If the mode is automatic, ARR is attempting to diagnose and restore the node. Manual diagnostics and/or restorals should only be attempted after inhibiting ARR and then killing any restorals initiated by ARR (see the procedure on the next page).

3.41 Nodes with ARR inhibited, with a maintenance mode of manual, or in-service nodes can be manually diagnosed. Refer to Table 4-S for the appropriate diagnostic and restoral commands to use for RPCNs, LNs, and DLNs.

3.42 A manually requested diagnostic typically results in the following sequence of events:

(1) The node under test is removed from service (OOS-NORMAL).

(2) The node under test is isolated (OOS-ISOLATED).

(3) Diagnostics are performed on the node under test.

(4) The node under test is usually unisolated (OOS-NORMAL).

(5) The node is not restored to service.

3.43 A manual conditional restore or an ARR requested conditional restore normally results in the following sequence of events:

(1) The node under test is removed from service (OOS-NORMAL).

(2) The node under test is isolated (OOS-ISOLATED).

(3) Diagnostics are performed on the node under test.

(4) The node is usually unisolated (OOS-NORMAL).

(5) If an overall All-Tests-Pass (ATP) resulted from the diagnostics, the node is restored to service (ACT-NORMAL).

To perform manual diagnostics on a node, the following steps should be performed:

(1) If the node's major state is OOS and its minor state for maintenance mode is AUTO, inhibit ARR using the **INH:DMQ** input message and stop any restorals initiated by ARR using the **STOP:DMQ** input message.

(2) If the node is an LN with a major state of ACT, manually remove the node's signaling link from service by changing the SLK's minor state to Manual Out-Of-Service with the **CHG:SLK** input message (**MOOS** keyword).

(3) Diagnose an RPCN node using the **DGN:RPCN** input message. To diagnose LNs, enter a **DGN:LN** request. To diagnose DLNs, refer to Table 4-S for the appropriate input message. Alternatively, the **RST:RPCN**, **RST:LN**, or the **RST:DLN** (only for 1A ESS switch) requests diagnostics to be run and on successful (that is, ATP) completion, conditionally restore the node to service.

(4) Any failing diagnostics (that is, a "Some Tests Failed" result) should be resolved until an ATP is achieved. Faulty circuit packs are to be replaced. When an ATP is achieved, go to Step 7.

(5) If the diagnostics are Conditional-All-Tests-Pass (CATP), determine the reason for the CATP. If the reason is "the node is not singly isolated," then perform the following:

— Unconditionally restore the node (see Step 7).

— Conditionally restore the adjacent nodes.

— After the adjacent nodes are restored, conditionally restore the original node from Step (a) and proceed to Step 8.

(6) If the diagnostic result is "NTR" or "ABT", determine the reason. Use the **OP:RING** input message (**DETD** keyword) to help determine the cause. Go back to Step 3 when the problem is cleared.

(7) If a DGN request is used, it is necessary to restore the node unconditionally using **RST:RPCN**, **RST:LN** or poke commands. For the 1A ESS switch use the **RST:DLN** input message to restore DLNs. A node should not be restored unconditionally unless one of the following conditions is met:

— A complete diagnostics produces an ATP response.

— A complete diagnostics produces a CATP response and the RI and NP minor states are both USBL.

(8) If the node is an LN, put the signaling link back into service by changing the SLK's minor state to in-service (IS) using the **CHG:SLK** input message (**IS** keyword).

3.44 When diagnostics produce a "Some Tests Failed" result, circuit packs should be replaced using the manual trouble location circuit pack list for the appropriate node type. 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:RPCN**, **RMV:LN**, or **RMV:DLN** (1A ESS switch only) input message. The node should then be isolated from the active ring with the **CFR:RING** input message (**EXCLUDE** keyword).

3.45 There are certain packs in each of the nodes which have Light Emitting Diode (LED) indicators on the front of the circuit packs. Table 4-T summarizes these indicators.

Table 4-T. Meanings of Circuit Pack LED Indicators

Pack Code and Type	LED Name	Meaning if Illuminated
UN123B Ring Interface 1	NT (No Token)	Node is not in active ring segment. Node is isolated or the ring is down.
TN922 Node Processor	RQ (Ring Quarantine)	Node is in the OOS maintenance state but could be in the active ring segment.
TN916 Link Interface	RQ (Ring Quarantine)	Node is in the OOS maintenance state but could be in the active ring segment.
TN1340 TN1641 Application Processor	ERROR	The application processor in the DLN has encountered an error.
UN303B/UN304 Integrated Ring Node	NT (No Token)	Node is not in active ring segment. Node is isolated or the ring is down.

3.46 Before any circuit pack is physically removed, the visual LED indicators should be inspected. It is desired that the node be OOS and isolated before any circuit pack is replaced. This should result in all of the RQ and NT LEDs being illuminated. If the node LEDs are not all illuminated after attempting to isolate the node, as a minimum, the LED indicators must appear as shown in Table 4-U.

Table 4-U. Circuit Pack Visual Indicators for Isolating Node

Pack to Be Replaced		LED(s) Which Must Be Illuminated
Code	Type	
UN122B/C	RI0	NT on the UN123B
UN123B	RI1	NT on the UN123B
TN922	NP	RQ on the TN922, or NT on the UN123B
TN916	LI	RQ on the TN916, or NT on the UN123B
UN303B/UN304	IRN	NT on the UN303B/UN304
TN915	PIFB	NT on the UN123B, or NT on a neighbor node UN123B that also contains a TN915
TN918	IFB	NT on the UN123B, or NT on a neighbor node UN123B that also contains a TN918
TN914	3BI	RQ on the TN922, or NT on the UN123B
TN69B	DDSBS	RQ on the TN922, or NT on the UN123B
495FA	Power	NT on the adjacent node's UN123B and NT on center node's UN123B
TN1803	PIFB	NT on the UN303B/UN304
TN1669	LID0	OOS on TN1669 or NT on UN303B/UN304

If there is a diagnostic failure in a node that cannot be solved by replacing packs on the diagnostic Trouble Locating Process list, the failing phase often lends a clue to the failure. The failing diagnostic should be investigated to determine the hardware being tested. It could be that a neighbor node is causing the failure.

3.47 An example of this would be a phase 1 failure. Part of phase 1 for all node types (that is, LN, DLN, RPCN) tests the ability of a message to be relayed from the BISO node, through the isolated node being diagnosed, to the EISO node. This type of failure could implicate the Interframe Buffer (IFB) or RI circuitry in either the BISO or EISO nodes. The recommended action is to diagnose the BISO and EISO nodes.

3.48 Another troubleshooting tip is to run diagnostics with the raw option. This allows all of the phases to run even if a failing phase is encountered. For example, running phase 2 in the event of a phase 1 failure could prove valuable in the determination of the faulty hardware. Phase 2 is the same as phase 1 except the tests are run from the EISO node.

3.49 When an equipment malfunction causes the fault recovery software to remove a node from service and places it in the OOS-NORMAL state, ARR attempts to diagnose the node and restore it to service. If ARR fails to restore the node, the node gets marked for manual action. Diagnostics should be run on the OOS node using standard diagnostic procedures.

3.50 If the node remains in the OOS-NORMAL state after the preceding actions, Small Scale Integration (SSI) circuit packs should be replaced in the following order:

(1) TN922 (NP)

(2) TN916 (LI) if applicable

(3) UN122B/C (RI0)

(4) UN123B (RI1).

3.51 When replacing these packs, care should be taken to ensure that no circuit pack is pulled unless the node is out-of-service and isolated. If replacing these circuit packs does not solve the problem, visually inspect the equipment for shorts, loose wiring, bent or broken pins, and proper cabling. If the problem persists, begin diagnostics on the adjacent nodes using standard diagnostic procedures.

Single Node Isolation

3.52 When an equipment malfunction causes the fault recovery software to isolate a node (OOS-ISOLATED), ARR attempts to diagnose and restore it to service. If diagnostics are ATP and ARR cannot restore the node to service, the node gets marked for manual action.

3.53 In this case, diagnose the node using standard diagnostic procedures. If the node remains in the OOS-ISOLATED state after correcting any failures found, the next step in clearing the isolated segment is to diagnose the BISO node. If the BISO node cannot be removed from the active ring because it is a small ring (that is, only four nodes), the **MOVFLT** option of the **CFR:RING** input message should be used to shift the isolated ring segment to encompass the BISO node.

3.54 If the BISO node is an LN, the signaling link state must first be changed to Manual Out-Of-Service (MOOS) with the **CHG:SLK** input message. The node can then be removed from service and excluded from the active ring with the **RMV:LN** command. When the BISO node is removed from service (OOS-NORMAL), it is automatically included in the isolated segment.

3.55 The next step is to diagnose the BISO node using standard diagnostic procedures. If the problem is associated with the BISO node and is corrected, the BISO node is included back into the active ring. The originally isolated segment can then be diagnosed and restored.

3.56 If the isolation still exists, the EISO node should be diagnosed in the same manner as the BISO node above. If the fault is found in the EISO node, the isolation should clear, leaving the original faulty node in the OOS-NORMAL state. The original faulty node can then be diagnosed and restored.

3.57 If isolation persists, replace all SSI circuit packs in the originally faulty node in the following order:

(1) UN122B/C (RI0)

(2) UN123B (RI1)

(3) TN915 (Padded IFB) or TN918 (Unpadded IFB)

(4) TN922 (NP)

(5) TN916 (LI) if applicable.

3.58 The next step is to perform a conditional restoral. If the isolation is not cleared at this point, perform a visual inspection of the affected equipment looking for shorts, bent or broken backplane pins, and cable problems. If everything looks in order, seek technical assistance.

Multiple Node Isolation

3.59 When an equipment malfunction causes the fault recovery software to remove multiple nodes from service and form an isolated segment around the faulty nodes, ARR attempts to diagnose and restore the nodes to service. If ARR fails to restore the nodes to service, the nodes are marked for manual action.

3.60 An example isolated node may look like Figure 4-8. Nodes ISO1 and ISO2 represent nodes in the isolated network that may or may not be faulty (that is, they may be innocent victims). The ISO0, ISO1, and ISO2 nodes may represent LNs or DLNs depending on whether the ring resides in the switch or the *A-I-Net* products STP. The ISO3 node represents an RPCN included in the isolated segment.

3.61 A suggested order to diagnose nodes until the segment is shortened is as follows: ISO0, ISO3, ISO1, ISO2, BISO, and finally, EISO.

3.62 The idea is to diagnose isolated nodes adjacent to the BISO and EISO nodes first. These nodes, ISO0 and ISO3 in Figure 4-8, are the suspected faulty nodes. When a problem is corrected and results in a shortened isolated segment, work within the new segment following the suggested order until all problems are resolved.

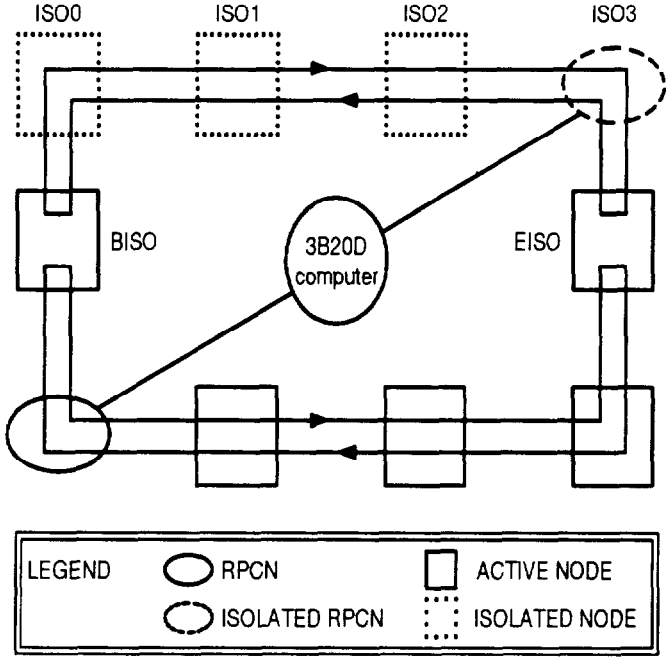


Figure 4-8. A Multiple Node Isolated Ring Segment

A. Down Ring

3.63 If an office carrying live traffic ever encounters a down CNI ring, restoring service as soon as possible is the prime concern. When this happens, verify with the **OP:RING** input message (**DETD** keyword) that the ring hardware is in fact down. The first recovery step is to perform a CNI/IMS Level 3 initialization using the **INIT:RING 3** (1A ESS switch and 4ESS switch), **INIT:CNI,LVL3** (5ESS switch), or **INIT:STP:LEVEL=3** (*A-I-Net* products STP) input messages.

3.64 If a CNI/IMS Level 3 initialization fails to establish an active ring, it may have already escalated to a CNI/IMS Level 4 initialization. If it has not escalated, perform a CNI/IMS Level 4 initialization using the **INIT:RING 4** (1A ESS switch and 4ESS switch), **INIT:CNI,LVL4** (5ESS switch), or **INIT:STP:LEVEL=4** (*A-I-Net* products STP) input messages.

3.65 If the ring hardware fails to initialize, scan back through the ROP printout for the initial stimulus which caused the ring to go down. Also, observe the failure messages that print out during the Levels 3 and 4 initializations. Pay particular attention to any **REPT RING TRANSPORT** errors that print out.

3.66 Because the ring does not initialize, there are probably multiple faults which have fragmented the ring so that no segment is long enough for use. Replacing all of the circuit packs in a suspect node may successfully remove one of the faults and allow the ring to initialize. The packs most likely to cause ring faults are the IFBs, RI0, RI1, and NP circuit packs.

⚠ CAUTION:
In a live ringdown escalation situation, use normal escalation strategy.

B. Unexplained Loss of Token

3.67 When RPCNs encounter a loss of token and no other node has come forth to identify the location of the ring problem, a ring transport error reports an unexplained loss of token. The EAR is automatically requested to test the continuity of the ring. If ring recovery cannot determine the location of the token loss, this error may continue to occur. It may be a transient error, or it may roll out in great frequency.

3.68 The probability of this error increases when there are OOS nodes or the ring has an isolated segment. This is due to nodes being hampered in their ability to report ring transport errors when they are OOS or the ring is reconfigured (that is, isolated segment).

3.69 If the loss of token occurs frequently, the solution is to isolate nodes one at a time until a configuration is found whereby the faulty node is no longer in the active ring.

C. Token Tracking Feature

3.70 Unforeseen problems in the CNI ring can cause the loss of the "token" message. The token tracking software feature was developed to assist in finding the lost token. The CNI hardware contains token tracking flip-flops in each node that toggles each time a token visits. The token tracking software is executed whenever token loss occurs. The IMS software interrogates the CNI ring collecting the data from the token flip-flops. The data then is analyzed and from the bit pattern the data identifies the vicinity of the token loss; however, this feature takes no recovery action. An output message is then sent to the ROP printer reporting the range of nodes in which the token was lost.

3.71 If token loss occurs frequently on the same node, while the whole ring is active, it is probably a hardware fault. Typically, the bad boards are ring interface (RI0 and RI1); but, Node Processor (NP) and Interframe/Intraframe Buffers (IFB) can also cause token loss.

3.72 With or without this feature, the CNI ring should recover automatically after the RPCN detects the token loss. However, the token loss will continue to occur until the source of the fault is eliminated.

Transient Faults

3.73 Transient faults can be difficult to find. If a ring has transient faults, it is a good idea to keep records on locations where the transient faults occur. This may tip off the start of failing hardware.

3.74 Always visually inspect the node. Look for unseated circuit packs, backplane damage, improper grounding, and unseated cable connections.

3.75 Diagnostics should be repeated to help bring out faults.

3.76 Applying light pressure to the front of the node or IFB circuit packs could stimulate a mechanically related intermittent fault to occur. Cracks in the backplane can be stressed by applying pressure.

3.77 Moving a node's circuit packs to another location on the ring may assist in finding the intermittent fault. Care should be taken on a live ring if packs are moved to another node. A small ring will go down if pulling packs causes breaks in the ring on the opposite sides.

3.78 If the transient faults occur, the problem may be with a **UN122** or **UN123** circuit pack. The following output messages will be displayed:

REPT RING TRANSPORT ERR
BLOCKAGE DETECTED b RAC c

REPT RING TRANSPORT ERR
RAC PARITY/FORMAT ERROR DETECTED b RAC c

REPT RING TRANSPORT ERR
TRANSIENT RAC ERROR DETECTED b RAC c

The faulty circuit pack may be determined by using the node identified in the **b** field of the output messages shown above. The **UN122**, **UN123**, or **TN915** at the node (field **b**) or the node on either side of the field **b** may be the source of the trouble. Replacing these circuit packs may resolve the transient faults.

General Tips and Cautions

3.79 Below is a list of general tips and cautions to be aware of at all times.

(a) Do not initiate Unconditional restorals on an isolated node unless it is certain no faults exist in the node. If a node or group of nodes are isolated due to a ring event, diagnostic phases 1 and 2 must be performed at a minimum. Otherwise, circuit packs could be uninitialized and cause blockage.

(b) Be careful not to leave ARR or Critical Node Restoral inhibited when the system is unattended. When the ring is fully operational, do not leave in manual mode.

(c) Do not allow a ring to operate with OOS nodes unnecessarily. Always take appropriate corrective action on faulty nodes.

(d) When analyzing ring transport errors, be aware of the real-time clock that prints out on these messages so that the order of events can be accurately determined. These error messages can be delayed when they print out on the ROP.

(e) When troubleshooting a ring-related problem, frequent use of the **OP:RING** input message (**DETD** keyword) to record overall ring status can benefit later ROP study.

(f) Save all error log files in /etc/log if a problem is likely to be escalated.

4. Application Processor Interface and Stream

4.01 The Application Processor System (APS), as shown in Figure 4-9, is an optional 1A Processor feature in the 1A ESS switch and is required in a 4ESS switch that provides access to a duplex 3B20D computer and its disk file subsystem. It consists of two Attached Processor Interface (API) units mounted in separate API frames and a duplex 3B20D computer equipped with up to eight drives. The duplicated API units interconnect the direct memory access channels of the 1A and 3B20D computer processors.

NOTE:
Reference to the 1A Processor also applies to the 1B Processor, where appropriate.

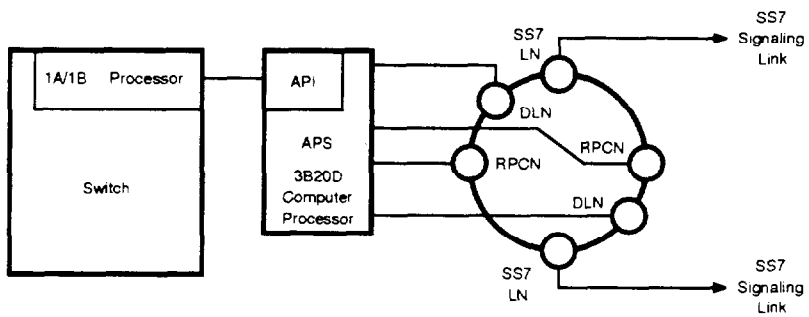


Figure 4-9. Application Processor System

4.02 The SS7 stream is comprised of three basic sections:

- 1A Processor to API
- API to 3B20D computer
- 3B20D computer to DLN.

4.03 The major causes for SS7 traffic stream outage are:

- 1A Processor outage
- 3B20D computer outage
- CNI ring outage
- Duplex API failure
- Duplex DLN failure.

Craft Notification

A. 1A ESS Switch

Displays/Pages

4.04 A STREAM alarm indicator is provided in the System Status Area of the APS display pages (top two lines of each page). When any part of the data stream is down, the STREAM indicator is lit and the SYS NORM indicator is no longer lit.

4.05 An SS7 Traffic Status Page (1109) is provided to report the status of the DLNs, 3B20D computer control units (CUs), APIs, and traffic stream. The stream flow direction and status are displayed graphically on this page. If any line is broken in an indicated direction, the stream is down in that direction. When the API is not scanning a stream direction, the API/CU connection is shown broken. When the DLN is not scanning a stream direction, the DLN/CU connection is shown broken.

Heartbeat Test

4.06 To determine the operational status of the SS7 traffic stream, a heartbeat message is initiated by the 1A Processor (every 250 ms) through the SS7 traffic stream to the active DLN. The message then travels around the CNI ring and returns back through the SS7 traffic to the 1A Processor. This test of the SS7 stream is typically transparent to the craft. When a heartbeat message is declared lost or late, the stream status bits are examined. If the stream is operational, no further recovery is attempted. If it is not operational, the stream is automatically restarted. The following messages are reported to the craft as shown in Table 4-V.

Table 4-V. Status Output Messages for Heartbeat Test

ROP	Output Message
1A ESS™ Switch Maintenance	CCS7 HEARTBEAT ALERT
APS	REPT DLNCM PROC (Strmfault): CCS7 HEARTBEAT ALERT

4.07 When a heartbeat message is declared lost or late for the second time in the 3-minute period, the stream status bits are looked at again. If the stream is operational, no further recovery is attempted. If it is not operational, the active API and DLN are restarted.

4.08 If a heartbeat message is declared lost or late for the third time in the 3-minute period, the stream is flushed. When this happens, the following messages are reported as shown in Table 4-W.

Table 4-W. Declared Lost or Late Output Messages

ROP	Output Message
1A ESS™ Switch Maintenance	CCS7 TRAFFIC STREAM OUTAGE
APS	REPT DLNCM PROC (Scanchk): CCS7 STREAM OUTAGE

4.09 If a heartbeat message is declared lost or late for the fourth time in the same 3-minute period, the active/standby DLNs are automatically switched.

4.10 Supplemental lost or late heartbeat messages are ignored until the 3-minute period expires. When the 3-minute period elapses, the counter is reset to zero. The next heartbeat message declared lost or late is treated as if it is the first. The cycle described above is repeated. Whenever the heartbeat message is successfully recovered, the following messages are reported as shown in Table 4-X.

Table 4-X. Recovery Output Messages

ROP	Output Message
1A ESS™ Switch Maintenance	CCS7 HEARTBEAT RECOVERED
APS	REPT DLNCM PROC (Strmfault): CCS7 HEARTBEAT RECOVERED

4.11 Whenever a stream outage is successfully recovered, the following messages are reported as shown in Table 4-Y.

Table 4-Y. Traffic Stream Recovery Output Messages

ROP	Output Message
1A ESS™ Switch Maintenance	CCS7 TRAFFIC STREAM RECOVERED
APS	REPT DLNCM PROC (Trafstrt): API SCANNING STREAM REPT DLNCM PROC (Scanchk): CCS7 TRAFFIC STREAM RECOVERED

ISUP Subsystem Check-In

4.12 The 1A Processor initiates an Integrated Services Digital Network User Part (ISUP) subsystem check-in message every 1 second. This message is sent through the SS7 stream to the active DLN. The DLN in turn routes it back to the APS. If the APS does not receive this message during two consecutive 2-second intervals, subsystem 3 (the ISUP subsystem) is declared out-of-service.

NOTE:
Other subsystems also check in.

When this happens, a Subsystem Prohibited (SSP) or SIPO message is sent to the local STPs to inform the network that ISUP communication is lost with the 1A Processor. The following message is reported on the APS ROP when this has occurred:

REPT SCMG
WARNING: SETTING ISDN-UP OUT OF SERVICE

4.13 When the subsystem check-in message is again received, a subsystem allowed message is passed to the local STPs and the following message is reported on the APS ROP:

REPT SCMG
ISDN-UP NOW BEING MARKED IN SERVICE

B. 4ESS™ Switch

Displays/Pages

4.14 A DLN/API Stream Status Page (1107) is provided to report the status of the DLNs, APIs, and traffic stream. The stream flow direction (mode) and status are displayed on this page.

Heartbeat Test

4.15 Like the 1A ESS switch, the 4ESS switch also has a heartbeat through the SS7 stream to the active DLN. The message then travels around the CNI ring and returns back through the SS7 stream to the 1A Processor.

4.16 When a heartbeat message is declared lost or late for the first time in a 3-minute period, the stream status bits are examined. If the stream is operational, no further recovery is attempted. If it is not operational, the stream is automatically restarted.

4.17 When a heartbeat message is declared lost or late for the second time in the 3-minute period, the stream status bits are looked at again. If the stream is operational, no further recovery is attempted. If it is not operational, the active API and DLN are restarted.

4.18 If a heartbeat message is declared lost or late for the third time in the 3-minute period, the stream is flushed. When this happens, the following messages are reported as shown in Table 4-Z.

Table 4-Z. Declared Lost or Late Output Messages

ROP	Output Message
4ESS™ Switch Maintenance	OP:RINGMNTR STREAM ACTIVE N
APS	REPT DLNCM PROC (Strmfault): LOST STRM THROUGHPUT

4.19 If a heartbeat message is declared lost or late for the fourth time in the same 3-minute period, the active/standby DLNs are automatically switched.

4.20 Supplemental lost or late heartbeat messages are ignored until the 3-minute period expires. When the 3-minute period elapses, the counter is reset to zero. The next heartbeat message declared lost or late is treated as if it is the first. The cycle described previously is repeated.

4.21 Whenever a stream outage is successfully recovered, the following messages are reported as shown in Table 4-AA.

Table 4-AA. Stream Recovery Output Messages

ROP	Output Message
4ESS™ Switch Maintenance	OP:RINGMNTR STREAM ACTIVE Y
APS	REPT DLNCM PROC (Trafstrt): API SCANNING STREAM

C. Subsystem Check-In

4.22 The 1A Processor on the 4ESS switch initiates an ISUP subsystem check-in message every 2 seconds. This message is sent through the SS7 stream to the active DLN. The DLN in turn routes it back to the APS. If the APS does not receive this message during two consecutive 2-second intervals, subsystem 3 (the ISUP subsystem) is declared out-of-service. When this happens, a Subsystem Prohibited (SSP) or SIPO message is sent to the local STPs to inform the network that ISUP communication is lost with the 1A Processor. The following message is reported on the APS ROP when this has occurred:

RING REPT SCMG
WARNING: SETTING ISDN-UP OUT OF SERVICE

4.23 When the subsystem check-in message is again received, a Subsystem Allowed message is passed to the local STPs and the following message is reported on the APS ROP:

RING REPT SCMG
ISDN-UP NOW BEING MARKED IN SERVICE

5. Maintenance Action as a Result of Stream Problems

5.01 Before attempting any manual recovery action, one should first determine the primary cause of the stream failure.

(a) Can the problem be in the 1A Processor or APS?

(b) What units are out-of-service?

(c) What was the sequence of events leading up to the stream failure?

Stream Status

5.02 If the stream appears operational but there is no data movement, request the stream status using the **OP:DLNCM** APS input message (**STREAM** keyword). The output from this request contains the stream status bits, receive buffer load/unload pointers, and send buffer load/unload pointers. The pointers control the data flowing into and out of the 1A Processor.

5.03 Normal data movement is observed by watching the load and unload pointers moving between multiple dumps of the header. During light traffic, the pointers may always be equal but have new values. This indicates data is passing through that section of the stream without delay. During heavy traffic it is normal for the unload pointer to trail behind the load pointer as the data is processed. In an overload condition, data is loaded into a buffer faster than it is unloaded, causing the load pointer to catch up to the unload pointer. This condition subsides when the traffic load is reduced.

5.04 When a load pointer equals the unload pointer and both pointers are not moving, a "no traffic" condition exists. This should normally not occur since the heartbeat and subsystem check-in messages constantly flow on the stream. On the 1A ESS switch, heartbeat messages can be inhibited (with input message **INH:PROGCTRL CS7HB**), but check-in messages are not controlled and only flow on the 1A Processor out stream. The stream is said to be "stuck" when the pointers are different but not moving, or the load pointer moves but the unload pointer does not. If the DLN's 1A Processor out unload pointer becomes stuck, eventually all 1A Processor out stream unload pointers stop moving as data backs up in the various buffers.

Manual Heartbeat

5.05 The 1A ESS switch provides a mechanism for the craft to manually request a heartbeat test. The input message associated with this is **TST-STREAM-**. The following messages (Table 4-AB) are output on the 1A Maintenance ROP depending on the results of the test. For additional information concerning these messages, refer to 1A ESS Switch IM/OM Manuals.

Table 4-AB. Heartbeat Test Output Messages

Test Result	Output Message
Success	CCS7 HEARTBEAT SUCCESS
Failure	CCS7 HEARTBEAT FAIL

Diagnostics

5.06 If there is a hardware fault causing the SS7 stream outage, more than likely it can be found in the active API or active DLN. If a fault occurs in either of these hardware units, the standby unit is made active while the active unit is put in standby mode. Fault recovery then runs diagnostics on the faulty unit and reports the results to the craft.

5.07 Since neither the 1A Processor nor the 3B20D computer has direct access to both sides of the API, diagnostic tests must be executed from each processor side of the API to completely test the API.

5.08 The craft can manually request API diagnostics from the 1A Processor side by using the **DGN:API** message. For the 1A ESS switch, this is found in the IM-6A001, *Input Message Manual.* For the 4ESS switch, this is found in the IM-4A001, *Input Message Manual.*

5.09 A 1A diagnostic request causes phases 1 through 9 to be executed. When phase 3 executes, a message is sent from the 1A Processor through the API to the 3B20D computer. This message requests the 3B20D computer to run the 3B20D computer set of API diagnostics. When the 3B20D computer diagnostics are completed, the 3B20D computer processor returns the results of its diagnostics to the 1A Processor. The 1A Processor then continues executing phases 4 through 9.

5.10 The craft can request API diagnostics from the APS by using the **DGN:API** message found in the 1A ESS Switch IM-6A002, *Input Message Manual,* or IM-4A001, *4ESS Switch/APS Input Message Manual.*

5.11 An APS diagnostic request causes the 3B20D computer processor to execute phases 1 through 12. These are the same phases that are run during 1A diagnostic phase 3. An additional 3B20D computer phase (phase 15) that tests the API interface to the off-line 3B20D computer CU may be requested.

5.12 The craft can manually request DLN diagnostics from the APS by using the **DGN:DLN** input message on the 1A ESS switch APS or the **DGN:LN** input message on the 4ESS switch APS. Refer to the IM-6A002, *1A ESS Switch/APS Input Message Manual*, or IM-4A001, *4ESS Switch/APS Input Message Manual*, for more information.

Manual Fault Recovery

5.13 If the SS7 stream is experiencing trouble and automatic fault recovery is not resolving the problem, one should seek technical assistance immediately. Repeated heartbeat failures could signal the start of a serious hardware/software problem. Failing diagnostics should be resolved as soon as possible. Faulty circuit packs and/or cables should be replaced as soon as possible. The standby unit should always be healthy in the event that it could be activated at any time.

5.14 If the APIs are duplex failed, the SS7 stream automatically restores to service as soon as one API is restored. No additional actions are necessary. If the APIs do not configure properly after a restoral attempt, removing and restoring API power resets their internal configuration and retries the restoral.

5.15 The 1A ESS switch and 4ESS switch tools that are provided to give the craft more control over the SS7 stream are shown in Table 4-AC.

Table 4-AC. Manual Fault Recovery Input Messages

Input Message	Maintenance Terminal	Tool Description
DGN:API	1A ESS™ Switch 4ESS™ Switch 1A/4 APS	Run diagnostics on specified API.
TEST:API TEST:API	1A ESS Switch 4ESS Switch	Test specified API.
RMV:API	1A/4ESS Switch	Remove specified API.
RST:API	1A/4ESS Switch	Restore specified API to service.
SW:APS	1A/4ESS Switch	Switch active and standby APIs.
DGN:DLN DGN:LN	1A APS 4 APS	Run diagnostics on specified DLN. Run diagnostics on specified DLN.
RST:DLN RST:LN	1A APS 4 APS	Restore specified DLN. Restore specified DLN.
SW:DLN	1A/4 APS	Switch active and standby DLNs.
TST-STREAM	1A ESS Switch	Test SS7 stream with a heartbeat message.
INIT:DLNCM, STREAM	1A/4 APS	Initialize SS7 stream.

WARNING:
Some of these requests may cause a brief service interruption. Automatic fault recovery should be allowed to correct detected trouble before manual intervention is attempted.

Maintenance and Diagnostic Documents

5.16 Refer to the following documents for specific information concerning maintenance and diagnostic for APS:

1A ESS 231-368-020, *APS—Operation, Maintenance, and Recovery User's Guide Processor Recovery Messages* (2 Volumes)

4ESS 254-200-100, *APS, 4ESS Switch Applications—Maintenance Reference Handbook*

6. Network Trouble

6.01 Events in the network sometimes have a direct impact on a particular switch. The reaction of the switch to a network event varies among switch vendors.

6.02 Network events can be categorized in two ways: those that affect call processing within a switch and those that do not affect call processing. Tables 4-AD and 4-AE provide a synopsis of these two network event categories and how the Lucent switching products alert the craft of the event. For a detailed description of each network indication, refer to the appropriate Lucent Technologies switch input/output manuals.

Protocol Problems

6.03 Protocol-related problems can be broken into three categories: protocol errors, inadequate protocol requirements, and vendor protocol violations. Protocol errors must be worked through the T1S1 committee or Bellcore for a change in requirements.

6.04 Inadequate protocol requirements result in one or more vendors interpreting protocol in a different manner than other vendors. These type of problems must be worked through the vendor(s) and addressed to the T1S1 committee for resolution.

6.05 A vendor protocol violation occurs when a vendor has implemented hardware and/or software that does not follow T1S1 protocol standards. The problem's solution is to refer the problem to the vendor for correction. For a list of Lucent Technologies documented protocol exceptions, contact your Lucent Technologies Account Executive.

6.06 The idea behind troubleshooting a protocol-related problem is to gather as much information as possible about it in order to determine which category it falls under. The appropriate action is then taken.

6.07 When possible, the following means are to be used:

- A protocol analyzer
- The Message Trap input request
- The **MON:SLK** input request
- The ROP printout.

6.08 For additional information concerning protocol problems, refer to Chapter 6, "Tools".

Table 4-AD. Indicators of Network Troubles Affecting Call Processing

Network Event	1A ESS™ and 4ESS™ Switches	5ESS® Switch
Signaling route congestion (TFC)	(1A/4E) MON:SLK message CCS7 TFC (flag X'00100) (1A) CCS7 MSG RETURNED REASON 3 dpc message (1A) TN08 messages when congestion level 2 or 3	MON:SLK message CCS7 TFC (flag H'00100)
Subsystem prohibited (SSP)	1A for subsystem 3 same as "Signaling Route Unavailable"	REPT CNCE C7SSPF message
Subsystem Allowed (SSA)	For subsystem 3 same as "Signaling Route Available"	REPT CNCE C7SSAF message
Signaling Route Unavailable	(1A) CCS7 POINT CODE FAILURE dpc (4E) TFP received REPT:MC3	CCS7 POINT CODE FAILURE dpc
Signaling Route Available	(1A) CCS7 POINT CODE RECOVERED dpc	CCS7 POINT CODE RECOVERED dpc
SLK Transmit Buffer Congestion	(1A,4E) REPT CNCE C7LCON[1X, 2X, 3X] message (1A,4E) REPT CNCE C7LCDIS[1X, 2X, 3X] message (1A,4E) REPT CNCE C7LCABM[1X, 2X, 3X] message (1A) TN08 messages when congestion level 2 or 3	REPT CNCE C7LCON[1X, 2X, 3X] message REPT CNCE C7LCDIS[1X, 2X, 3X] message REPT CNCE C7LCABM[1X, 2X, 3X] message
Loss of All Local SLKs	(1A,4E) REPT CNCE C7SPI message for adjacent STPs (1A) CCS7 POINT CODE FAILURE dpc (4E) TFA received - REPT:MC0	REPT CNCE C7SPI for adjacent STPs REPT CNI RING condition = all links down
DLN Congestion	(1A,4E) REPT DLN CNGST	REPT DLN CNGST
Loss of All DLNs	(1A,4E) RING/STREAM STATUS indicators: 1A ESS Switch - Page 1109 4ESS Switch - Page 1107/1108 (1A,4E) REPT DLNCM-STDLN: NO ACTIVE OR STANDBY DLN (1A) CCS7 TRAFFIC STREAM OUTAGE (1A) CCS7 HEARTBEAT ALERT	MCC Page 118 indicators REPT CNI RING condition = DLN unavailable status = direct signaling oos status = trunk signaling oos status = tcap signaling oos REPT RINGMON DLN ERROR = (hbllmprob or hbtofail or hbnact)

Table 4-AE. Indicators of Network Troubles Not Affecting Call Processing

Network Event	1A ESS™ and 4ESS™ Switches	5ESS® Switch
Signaling Link (SLK) Unavailable	(1A,4E) REPT CNCE C7ACOCOV or C7ACOCER message	REPT CNCE C7ACOCOV or C7ACOCER msg
SLK Available	(1A,4E) REPT CNCE C7ACB message	REPT CNCE C7ACB message
Signaling Route Restricted (TFR)	(1A,4E) MON:SLK message CCS7 TFR (flag X'00100)	MON:SLK message CCS7 TFR (flag H'00100)
Signaling Route Unavailable (TFP)	(1A,4E) MON:SLK message CCS7 TFP (flag X'00100)	MON:SLK message CCS7 TFP (flag H'00100)
Signaling Route Available (TFA)	(1A,4E) MON:SLK message CCS7 TFA (flag X'00100)	MON:SLK message CCS7 TFA (flag H'00100)
Route Congestion Test (RCT)	(1A,4E) MON:SLK message CCS7 RCT (flag X'00040)	MON:SLK message CCS7 RCT (flag H'00040)
Signaling Processor Outage (SIPO)	(1A,4E) REPT CNCE C7POR message	REPT CNCE C7POR message
SIPO ended	(1A,4E) REPT CNCE C7PORE message	REPT CNCE C7PORE message
Adjacent STP Signaling Isolation	(1A,4E) REPT CNCE C7SPI message	REPT CNCE C7SPI message
Loss of 1 DLN	(1A,4E) REPT DLNCM PROC: SWITCH DLNS (1A ESS Switch) Page 1106 and 1109 indicators (4ESS Switch) Page 1106 and 1107 indicators	REPT RINGMON DLN ACTION = switch complete
SLK Receive Buffer Congestion (SIB) sent	no indicator	no indicator
SIB received	no indicator	no indicator

7. CNI Internal Data Base Trouble

7.01 The CNI provides three types of audits for detecting and correcting CNI internal data base troubles. These are described in this part: the LKNODE, NIDATA, and NMDATA families of audits.

7.02 Other audits may be provided by applications for detecting troubles in application data bases. The *A-I-Net* products STP provides three application audits: STPDAT, RT7TAB, and SCRDAT. These will be described later in this section.

7.03 When a data base trouble is suspected, the appropriate audit should be executed and the output used to manually correct the trouble as necessary. If a scheduled audit detected an error, its output should be analyzed to determine what manual corrections are needed. It is important to note that most audits are *correcting* audits (no manual corrections are necessary).

7.04 Where provided, specific data on audit errors can be used to identify the suspect software or hardware causing the data base trouble. Even if the errors are automatically corrected, recurrent error correction by the same audit indicates some problem outside the scope of the audit. This is where patterns of problems can lead to a solution.

7.05 The major items to check on audit messages and reports are:

- The types and frequencies of specific errors encountered, particularly if an audit unexpectedly starts reporting numerous errors.
- Which errors are corrected, which errors are not corrected, and how many are found.
    - The *UNIX* RTR Operating System Plant Measurements Common Report (PMCR) will indicate how many errors are found by each audit. If an audit runs automatically and finds no errors, there is no printout associated with the audit. Table 4-AF shows the input and output messages associated with the *UNIX* RTR Operating System PMCR.

Table 4-AF. Data Base Audit Messages

Switch	Input Message	Output Message
1A ESS™	**OP:PMCR**	**OP PMCR REPORT**
4ESS™	**OP:PMCR**	**REPT OP PMCR**
5ESS®	**OP:PMCR**	**REPT OP PMCR**

Refer to the appropriate switch's input and output manuals for more information concerning these messages.

- Whether or not particular audits aborted or completed.
  - If these problems cannot be identified easily, they should be investigated further.
- Changes in the state of particular units made suspect by audit errors.

NOTE:
A particular audit taking a long time to complete is not necessarily an indication of problems. When an audit is manually requested, it may or may not execute immediately. Since audits are considered low-priority work, in a busy office, an audit may be deferred a significant length of time. Also, because most audits check office-dependent data structures, the amount of time required to run depends on how the office is equipped.

7.06 Although most CNI data base troubles are reported to the user via **AUD** output messages, there are other messages that should be used to analyze data base troubles. Some of these messages are produced in response to manual requests while others are generated automatically. There are basically four types of output of interest: **AUD** and other audit-related output messages, the Plant Measurements Common Report audits section, Processor Recovery Messages, and other messages caused by data base troubles. By correlating the information provided by these messages and reports, patterns of problems can be identified.

Link Node Data Audit (AUD:LKNODE)

7.07 This is an internal data audit of a specific link node; it verifies the recent changeable data associated with the node. The audit does the following:

(1) Compares certain data tables in the 3B20D computer memory with disk data and reports any mismatches.

(2) Checks for invalid data within the tables and inconsistencies across tables.

(3) If the central processor data is error free, checks the corresponding data in the node.

(4) Automatically corrects any errors uncovered if the errors cannot be corrected via recent change.

(5) Outputs unique error codes so that manual recent changes can be used to correct any other errors.

7.08 Before running this audit, specify the link node to be audited with the **SET:SLK** message. Then, initiate the audit with the **AUD:LKNODE 1** message for the 1A ESS switch and 4ESS switch or the **AUD:LKNODE=1** message for the 5ESS switch.

Internal Data Audits (AUD:NIDATA)

7.09 These are audits of all recent changeable data in the 3B20D computer. Each audit does the following:

(1) Compares the tables contained in the 3B20D computer memory with tables maintained on disk and reports any mismatches.

(2) Checks for invalid data within a table and inconsistencies across tables.

(3) If any errors are uncovered which cannot be corrected via recent change, automatically corrects the errors.

(4) Outputs any other errors (using a unique error code) so that manual recent changes can be used to correct the errors.

7.10 These audits can be manually initiated by typing in the following input message:

- **AUD:NIDATA** *x* (for the 1A ESS switch and 4ESS switch)
- **AUD:NIDATA=***x* (for the 5ESS switch and *A-I-Net* products STP).

where *x* is the number of the specific audit to be run.

7.11 Table 4-AG cross-references each NIDATA audit member with the corresponding CNI data view/functions.

Table 4-AG. Data Corresponding to NIDATA Audit Members

Audit Member	1A ESS™ Switch 1105 Page Function	4ESS™ Switch DMS Function	5ESS® Switch RC View	*A-I-Net*® STP
1	ofdata	ofdata	15.1	—
2	lkdata	lkdata	15.2	—
4	route	lsrout, clsrout	15.9	—
5	setssn	—	15.10	tninfo
8	gbltt	gttran	15.11	—
9	route	lsrout, clsrout	15.12, 15.13	—
10	rcptp	—	15.14, 15.151 5.16, 15.17 15.18	rcptp

7.12 It is suggested that these audits be run daily to ensure the reliability of the CNI data base, and after each recent change activity to audit the success of the session. It is not necessary to run these audits after each recent change order; rather, once after all recent change activity for a session is sufficient. Any unresolved errors found should be referred to appropriate personnel using local practices.

A. Office Identification Data (NIDATA Audit 1)

7.13 The office identification data consists of the local region, the local function number, the local point code, the international local point code (for International Switching Centers only), the function number of the destination for link integrity status messages, and the local *Common Language* CLLI code.

7.14 This audit checks the above data for: correct version number, mismatches between the 3B20D computer memory and disk, and invalid data. It also cross-checks it with corresponding link configuration data.

B. Link Configuration Data (NIDATA Audit 2)

7.15 The link configuration data consists of attributes for each signaling link and its far-end network entity.

7.16 This audit checks the above data for mismatches between the 3B20D computer memory and disk, and invalid data. It also cross-checks it with corresponding office configuration data.

7.17 For each of the linksets mentioned in the link configuration data, the audit cross-checks the corresponding linkset to ring node address (rna) and linkset relation data. The 'Indata' directory is checked for extraneous files.

C. Cluster/Member (Point Code) Routing Data (NIDATA Audit 4)

7.18 The cluster/member routing tables map an SS7 point code to a linkset. It consists of data for each cluster and each cluster member.

7.19 This audit checks the above data for mismatches between the 3B20D computer memory and disk, and invalid data. It also cross-checks it with corresponding link configuration data.

7.20 The audit checks the data in the member information table for validity and mismatches between the 3B20D computer memory and disk.

D. Subsystem Data (NIDATA Audit 5)

7.21 The subsystem distribution and local subsystem tables provide message discrimination information to be used by the subsystem manager. Data provided for each subsystem includes destination channels and addresses for messages, the index of the function to dispatch for message handling, and the point code and subsystem number of the mate subsystem, where applicable.

7.22 This audit checks the above data for mismatches between the 3B20D computer memory and disk, and invalid data.

E. Permanent Relation Data (NIDATA Audit 6)—STP Only

7.23 The permanent relation table is a list of the point codes and associated subsystems which are to be notified about certain network events. For each point code, there may be multiple subsystems associated with it.

7.24 This audit checks the above data for mismatches between the 3B20D computer memory and disk, and invalid data.

F. Global Title Translator (NIDATA Audit 8)

7.25 A Lucent Technologies switch addresses Signaling Connection Control Part messages to STPs for Global Title Translation (GTT). The GTT table indicates which STP pair performs GTT for a certain service.

7.26 This audit checks the above data for mismatches between the 3B20D computer memory and disk, and invalid data.

G. Network Identifier Routing Information Data (NIDATA Audit 9)—5E8 and Earlier

7.27 The network identifier routing data contains the routing flag, preferred linkset, and director index. Both tables are used for routing to the appropriate SS7 network.

7.28 This audit checks the above data for mismatches between the 3B20D computer memory and disk, and invalid data. It also cross-checks it with corresponding director index-to-network identifier data.

⇒ NOTE:
This function is performed by NIAUDIT 4 starting with 5E9.1.

H. Protocol Timers and Parameters Data (NIDATA Audit 10)—5E9.1 and Later

7.29 The RCPTP function provides for the changing of timers, parameters, and thresholds (identified in Chapter 3). The values used as input must be within CNI defined ranges.

7.30 This audit checks the above data for mismatches between the 3B20D computer memory and disk, and for invalid data.

Network Management Audit (AUD:NMDATA)

7.31 These audits are controlled by the System Integrity Monitor. They are concerned with the integrity of network management dynamic data.

7.32 These audits run in either error detection mode or error correction mode (user specified). For applications that have CNI routing data maintained in processors other than the 3B20D computer, the remote copy of the data is updated if the audit corrects errors.

7.33 The appropriate Lucent Technologies product customer support group should always be notified of NMDATA audit errors. Initiate the desired audit by entering the following input message:

- **AUD:NMDATA** *x* (for the 1A ESS switch and 4ESS switch)
- **AUD:NMDATA=***x* (for the 5ESS switch and *A-I-Net* products STP).

where *x* is the number of the specific audit to be run.

A. Routing Data Linked List and Consistency Check (NMDATA Audit 1)

7.34 The routing data linked list is used to manage the dynamic routing information as different network events occur (such as remote link failure or congestion). This audit checks for errors in these tables, including discrepancies between different fields in a specific routing table entry.

7.35 Since correction mode suppresses point code state changes and since state changes must normally occur as part of CNI operation, it is recommended that the audit be manually run only in detection mode.

B. Load Share Tables (NMDATA Audit 2)

7.36 The loadshare table data is used for message routing link selection in the direct link node, the D-Channel node, and the 3B20D computer. This audit checks for errors in that data. The audit can be run in error correction mode with no adverse side effects.

C. Route Set Test Table (NMDATA Audit 3)

7.37 The NMDATA 3 audits the (cluster) Route Set Test (RST) tables based on the routing table. The purpose of this audit is to ensure that the point code (or cluster) is properly associated with the route set test procedure. The (cluster) route set table is used by CNI internally and resides in the 3B20D computer only.

A-I-Net Products STP Internal Data Base Audits (AUD:STPDAT)

7.38 These are manually initiated audits of the *A-I-Net* products STP recent changeable data base. Each audit does the following:

(1) Compares certain data tables in the 3B20D computer memory with disk data and reports any mismatches.

(2) Checks for invalid data within the tables and inconsistencies across tables.

(3) If the central processor data is error free, checks the corresponding data in the nodes*.

(4) Automatically corrects any errors uncovered, if the errors cannot be corrected via recent change.

(5) Outputs unique error codes so that manual recent changes can be used to correct any other errors.

---

* This is done with a ring broadcast message containing the correct data. Only the concerned nodes audit the data; all other nodes ignore the message. The nodes correct any errors found and send responses back to the 3B20D computer to report the errors.

7.39 The STPDAT audits can be requested either by the **AUD:STPDAT** input message or the 1143 display page.

If requested manually with the Detailed option, up to 255 detailed reports are provided. These reports contain an error code and description of the error encountered. The four data words in the output message do not provide any additional information (they are always zero). The length of time these audits run depends on the size of the associated data base tables.

A. Domain Nonzero Routing Table (STPDAT Audit 2)

7.40 In the domain nonzero routing table, each domain and A field combination either maps directly to a route number (for 3-digit translation) or points to a supplementary routing table (for 6-digit translation). This audit cross-checks the above data with data in the supplementary information table and route information table. It checks that those domain nonzero entries with a route number have a valid route number. Likewise, those entries which require a supplementary routing table should be marked as such in that table.

B. Supplementary Routing Table (STPDAT Audit 3)

7.41 This audit scans through the supplementary information table and checks that all of the supplementary routing tables are set up accordingly. For example, each of the routes in a supplementary routing table must be valid and must be assigned in the route information table.

C. Office Identification Data (STPDAT Audit 6)

7.42 This audit checks the validity of the data items which are used to describe the location of this office in the network. These items include the local function number, local CLLI code, local point code, and aliases. This audit cross-checks the above data with corresponding link configuration data. Also, the alias data is cross-checked with the cluster/member tables and pool to point code table. If a particular data item mismatches between the disk and main memory copies, no further checking of that item is normally done. The audit continues with the next data item to be checked. The self-identification data in the link node is checked by the **AUD:LKBDST** audit.

D. Link Configuration Data (STPDAT Audit 8)

7.43 Each link has its own set of data which describes the characteristics of the link (for example, link speed, link type), the connectivity of the link, and the linkset assignments for the link. This audit checks the validity of the data which describes each link in the office. The link data is also cross-checked with office identification data, the appropriate linkset assignment tables, and, if the link is designated for screening, the corresponding screening data. The link configuration data in the link node is checked by the **AUD:LKBDST** audit.

E. Protocol Timers and Parameters (AUD:STPDAT=10)

7.44 The AUD:STPDAT 10 detects and corrects inconsistencies and errors with the protocol timer and parameter data in 3B memory and in the disk file. The audit checks for data range errors, cross-parameter inconsistencies, and inconsistencies with 3B memory and the disk file. Data range limits and cross-parameter requirements are listed in the Database Administration Manual description for the **timthr** function.

F. Translation Number Information Table (AUD:STPDAT=11)

7.45 The translation number information table contains all the translation numbers currently assigned and routing information concerning each translation number. Each is assigned a translation type, a primary point code and subsystem number, and a cost. If the translation type is duplex, the entry also contains a secondary point code and subsystem number, a secondary cost, and a mate translation number. This audit verifies this data and cross checks it with corresponding data in the route information table (each translation number is assigned as a route type 9). It also ensures that mated translation numbers refer to each other. This audit should follow the route information table audit.

If no mismatches are reported between the main memory and disk versions of the data, the translation information table data is audited in the appropriate link notes.

G. Ordered Route Table (STPDAT Audit 12)

7.46 The ordered route table provides a translation from a given destination point code to an outgoing linkset to that destination along with relative cost of the outgoing linkset. Note that a point code may have multiple entries in this table. The routing data is contained in basically four tables: the ordered route table, the cluster/member table, the member information table, and the populated cluster bitmap.

⇒ NOTE:
Routing data for all remote clusters and local clusters and members known to this office is maintained by both CNI and *A-I-Net* products STP software. This audit cross-checks between the two and reports any errors. The cluster routing data referred to here includes data for both local and nonlocal networks.

7.47 For each ordered route table entry, this audit also verifies the corresponding link configuration data, the alias list (a list of alias point codes or capability codes), and the populated cluster bitmap. Member routing data for populated clusters is cross-checked with corresponding pool and point code data, corresponding link configuration data, and the alias list.

7.48 This audit also checks the consistency and validity of the data in the NID and small network index tables. If the above checks find no errors, the populated cluster bitmaps in the SS7 link nodes are checked.

H. Ordered Global Title Translation (STPDAT Audit 13)

7.49 The ordered Global Title Translation (GTT) data is maintained in four tables: domain nonzero routing, supplementary routing, route information, and translation information. The data allows the *A-I-Net* products STP to translate a given Global Title type and address combination to the appropriate destination point code and subsystem. This audit verifies the data in all the tables as described below.

7.50 The domain nonzero, supplementary routing, and supplementary information tables are verified for every possible global title type and address combination. These tables are then searched for assignment translation numbers. For each one found, the corresponding data in the route information and translation information tables is verified and cross-checked.

I. Linkset Assignment & Designated Destination Data (STPDAT Audit 14)

7.51 For each assigned linkset number, this table specifies the linkset name (that is, 2-6 code), the link type, and far-end signaling point information (that is, point code, CLLI code, and even/odd STP identifier). This data is a composite of the links making up a particular linkset. This audit verifies the data and cross-checks it with corresponding link configuration data, self identification data, and concerned signaling point data for B/D-links.

J. Special Studies Table (AUD:STPDAT=15)

7.52 The special studies data specifies for which messages and linksets the special studies measurements should take. This data contains: the incoming linkset number, a special study number (up to 10 per linkset), originating point code (OPC), destination point code (DPC), and service information octet (SIO).

K. Concerned Signaling Point Data (STPDAT Audit 16)

7.53 The concerned signaling point data (also known as the broadcast list) is a list of point codes used when sending broadcast messages to adjacent offices. This audit verifies the data and cross-checks it with corresponding self identification data (that is, the alias list) and linkset assignment data.

L. Limited TFP Broadcast List (AUD:STPDAT 17)

7.54 This audit scans through the Limited TFP Broadcast List in 3B memory. It compares each entry with the corresponding one in a disk file to ensure a match between corresponding entries in memory and disk. The version number of the disk file must also match a version number stored in memory. In the event that the disk file does not exists, it will be created from the information in memory. The audit then terminates.

M. Map Translation Type Data (AUD:STPDAT=18)

7.55 This audit checks for mismatches and data validity in the Mapping Link Set Identifier and Translation Type Mapping tables. The SCCP message translation type, 3-digit table number, mapped translation type, and Originating Point Code (OPC) data in the disk files are compared with the data in the 3B20D shared library.

7.56 The audit opens the disk files. If they cannot be opened, the error is reported and a new disk file is built from the current version of the file in the 3B20D file. The audit will be terminated if:

- The disk file is the wrong size
- The read fails
- The version number of the read does not match.

7.57 If the read is successful, the data of the disks and the 3B20D are checked. If there is a mismatch in *ANY* entry, the errors are reported. If all table entries are matched between the disk and 3B20D shared library, then data integrity checks are made.

7.58 If no errors occur from these data/integrity checks, messages containing the Mapping Link Set Identifier and Translation Type Mapping tables information is broadcast to all SS7 notes. If an error is received from the node, it is reported to the System Integrity Monitor (SIM).

A-I-Net Products STP Full Gateway Screening Audits (AUD:SCRDAT)

7.59 The **AUD:SCRDAT** audits are responsible for intertable validity checking and for ensuring the general integrity of the *A-I-Net* products STP office level Full Gateway Screening data base. If any inconsistencies in data are found during an audit, explicit **AUD SCRDAT** error messages are generated on the ROP and the errors themselves are corrected. The specific audits are shown in Table 4-AH.

Table 4-AH. SCRDAT Audit Members

Audit Member	Description
1	This member audits the linkset files for out of range fields, loops in the binary trees, and performs validity checks on the Next Screening Function Indicator (NSFI) fields. Additionally, it performs cross-checks on the NSFI and Next Screening Reference Index (NSRI) branches between tables. Finally, this audit cross-checks the linkset data between the "index to reference" and "reference to index" tables as well as between the Called Party Address (CDPA) map data, the linkset and office data.
2	This member compares the data in the linkset disk files to that in the signaling links.
3	This member compares 3B20D computer resident screening data to the corresponding disk resident data.
4	This member compares the linkset files and the corresponding office data files.

7.60 For further reference on using **AUD:SCRDAT**, refer to 270-750-404, *A-I-Net STP Input Message Manual*, and *270-750-405, A-I-Net STP Output Message Manual.*

Measurements

5

Contents Page

Contents Page

Contents Page

Measurements

5

1. Common Network Interface Performance Traffic Reports

Introduction

1.01 The Common Network Interface (CNI) performance traffic reports, referred to in this document as CNI measurement reports, will consist of CNI and application measurement data. The CNI allows reports that present measurement data in either a fixed or a flexible format. The reports described here are fixed format and cannot be altered by the user. Individual sites may wish to use the flexible format feature to create reports for specific uses not adequately addressed by the fixed-format reports. Such reports may include application-specific measurement data collected by CNI. In particular, many of the measurements apply only to *A-I-Net*® advanced intelligent network products Signal Transfer Point (STP). For information concerning flexible format options, refer to the following documents:

- 231-390-500, *Common Channel Signaling 7, General Description, Feature Document, 1A ESS Switch*
- 234-100-120, *Common Channel Signaling System—CNI 4ESS Switch*
- 235-190-120, *5ESS Switch Common Channel Signaling Services Features*
- 270-750-406, *A-I-Net STP Data Base Administration.*

1.02 All reports have a header section at the top of the report providing identifying information about the reporting office (such as the *Common Language** CLLI code and generic software).

⇒ NOTE:
Refer to the appropriate document for the generic software release you are using.

1.03 The body of the report contains data that is derived from measurements. This data is useful in identifying problems and in troubleshooting faults as well as Engineering and Administration. The measurements can be peg counts, durations, or thresholds.

1.04 Since some of the measurements are generated per link or per node, it is sometimes necessary to accumulate the measurements to derive a useful value for output to users. Other measurements may be derived via specialized algorithms. When analyzing these reports, the user should consider how the data is derived. Users of measurement data are located both on-site and at various support system centers. Therefore, reports are output to both on-site and remote users. The Measurement Output Control Table (MOCT) controls the output of all CNI measurement reports. Users on-site can demand any reports at any time with the **OP:SMR** input message. Reports for remote support system users, however, are often polled (that is, generated and stored for later retrieval). These reports are intended for later output upon request by the support system.

1.05 There are four important CNI reports discussed in this section:

(a) Signaling Network Performance Report, Part 1 (SNPR1)

(b) Signaling Network Performance Report, Part 2 (SNPR2)

(c) Machine Performance Report (MPR)

(d) 30-Minute Marginal Performance Report (30MPR).

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

1.06 The layouts and the measurements contained therein reflect the following generic software releases as shown in Table 5-A.

Table 5-A. Generic Software Release for CNI Reports

1A ESS™ Switch ®STP APS	4ESS™ Switch APS	5ESS® Switch	*A-I-Net*
1AP3F	4AP14 or later	5E9 or later	Rel 2 or later

1.07 If the application software release is not one of those listed in the preceding table, refer to the output manual(s) listed below for the appropriate **REPT SMR** layout and measurements:

- OM-6A002, *1A ESS Switch/APS Output Message Manual*
- OM-4A001, *4ESS Switch/APS Output Message Manual*
- 231-390-500, *Common Channel Signaling System 7, General Description, Feature Document—1A ESS Switch*
- 234-100-120, *4ESS Switch Common Channel Signaling System, Common Network Interface*
- 235-190-120, *5ESS Switch Common Channel Signaling Services Features*
- 235-600-750, *5ESS Switch Output Message Manual*
- 270-750-405, *A-I-Net STP Output Message Manual*
- 270-750-406, *A-I-Net STP Data Administration*

⇒ NOTE:
Portions of some reports may contain information not related to SS7. Refer to the appropriate Output Message Manual above for information on Non-SS7 measurements.

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

2.01 The SNPR1 is a total office report that is collected every 5 minutes and printed out automatically each hour, and once for the entire day. The data coverage should be 012/012 (that is, twelve 5-minute periods) for the hourly reports and 288/288 (that is, 288 five-minute periods) for the daily report. This report provides an overall view of signaling performance for the office. It is especially helpful in link engineering and in central processor engineering.

2.02 The SNPR1 does not provide detailed measurements for each link. In fact, the data on this report cannot be directly used to determine the condition of any specific piece of hardware. Instead, it shows cumulative counts for the entire office. This report can be used to determine general performance of the office in the areas of:

- Signaling load handled
- Signaling Link (SLK) failures experienced
- Signal unit errors detected
- Number of message transfer failures.

2.03 This report should be checked daily for counts indicating poor link performance. The hourly reports from any periods should be compared for trends and abnormalities. Frequency of problems should also be examined. A high count on one report is not necessarily an indication of a problem. On the other hand, the same count(s) occurring at the same time each day may point to externally induced problems. If the lack of adequate link node buffer capacity has caused past link congestion, then this report should be checked daily to prevent link congestion events. If problems are indicated, the user should then refer to the SNPR2 or 30MPR reports for detailed measurements of specific links.

2.04 The basic layout of the report is shown in Figure 5-1.

Report Output Format

```
xx REPT SMR ASNPR1HR STARTED
SIGNALING NETWORK PERFORMANCE REPORT - PART I

REPORTING OFFICE: local CLLI code  REPORT INTERVAL: hourly or daily
CURRENT GENERIC: gen_id            AUTOMATIC REPORT
DATE: yy/mm/dd,  TIME: hh:mm:ss
REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
DATA COVERAGE: 012/012

   SIGNALING LOAD ---            RECEIVED     TRANSMITTED
    CCS7 MSU BYTES:               BYMSUR          BYMSUX
    CCS7 ROUTED MSGS:             MGMSUR          MGMSUX
    TOTAL GTR MSGS REC'D:        SC7RGTR

   SIGNALING PERFORMANCE ---                                  PEG          TIME
                                                             COUNT        (SEC.)
    CCS7 PERFORMANCE ---                                     -------      -------
       SIGNALING POINT ISOLATION                              SPISP       SPISPT
       LINKSET FAILURE                                       CLFSP       CLFSPT
       SIG LINK CONGESTION ONSET (LEVEL 1)                 L7LCON1X    L7LCON1XT
       DECLARED LINK FAILURES                                L7FLD       L7FLDT
       AUTOMATIC CHANGEOVERS                                 L7ACO
       RECEIVE BUFFER OVERFLOW                              L7BOFR
       RECEIVE BUFFER OVERLOAD                              L7BOLR      L7BOLRT
       TRANSMIT BUFFER DISCARD LEVEL 1                    L7LCDIS1X
       ROUTING AUDIT FAILURES                              L7RTGAUD
       ALTERNATE LINK SET ROUTING TRANSITIONS
       EXCEPTION REPORTS (THRESHOLDS EXCEEDED) ---         LN7ALSR
          ERRORED SECONDS                                   ERSECTE
          DETECTED ERRORS                                   CRCERTE
          BYTES RETRANSMITTED                               BYRXTE
          AUTOMATIC CHANGEOVERS                            L7ACOTE
       MESSAGE TRANSFER FAILURES ---
          ECIS6 MSGS DROPPED - RPC CONGESTION           DRPEMSG1+2+3
          MSUS DISCARDED - ROUTING DATA ERROR               L7BADRTG
          LOOPING CCS7 MSGS                                 MSG7LOOP
          GTT REFUSED - BLOCKED                              GTTUNBC
          GTT REFUSED - NO TRANSLATION                       GTTUNNT
          SIG LINK MESSAGES DISCARDED                   MSUDISC0+1+2
          MSGS DROPPED - RPC CONGESTION                 DRP7MSG1+2+3
          SCCP MSGS - UNKNOWN ADDRESS       (LN7)          SC7RERUA
          SCCP MSGS - UNKNOWN ADDRESS TYPE (LN7)        SC7RERUATY
          SCCP MSGS - UNEQUIPPED SUBSYSTEM (LN7)         SC7RERUNE
          SCCP MSGS - UNKNOWN ADDRESS       (OFC)          SCRERUA
          SCCP MSGS - UNKNOWN ADDRESS TYPE (OFC)        SCRERUATY
          SCCP MSGS - UNEQUIPPED SUBSYSTEM (OFC)         SCRERUNE
          SCCP MSGS - PROHIBITED SUBSYSTEM (OFC)         SCRERPRO

xx REPT SMR ASNPR1HR COMPL
```

Figure 5-1. Layout of the SNPR1 Report

Signaling Load

2.05 This section of the report shows the number of messages received and transmitted for various types of messages found on Signaling Common Channel System 7 links. The octet counts are for Message Signal Units (MSUs) only (flags FIUSs and LSSUs are not counted).

2.06 Measurements in this section are defined as follows:

BYMSUR The number of octets in messages received that contain Signaling System 7 (SS7) message data (called message signal units)

BYMSUX The number of message signal unit octets transmitted, not including retransmitted messages

MGMSUR The number of MSUs received (essentially a count of all received SS7 traffic messages)

MGMSUX The number of MSUs transmitted (essentially a count of all transmitted SS7 traffic messages)

SC7RGTR The number of received global title messages.

Signaling System 7 Performance

2.07 This section of the report indicates failure conditions such as Signaling Point Isolations (SPIs), buffer congestion, link failures/changeovers, link errors, translation failures, and message transfer failures. These counts and thresholds are for error conditions that indicate poor link performance.

NOTE:
The SNPR1 report does not provide time of day information for congestion events. Refer to the critical event messages or log file for that information.

2.08 Measurements in this section are defined as follows:

BYRXTE The number of times the BYRX count exceeded threshold value.

CLFSP Cumulative total of all linkset failures in the office.

CLFSPT The duration of the CLFSP.

CRCERTE The number of times the cyclic redundancy check error (CRCER) count exceeded threshold value.

DRP7MSG1 The number of priority Level 1 messages discarded because of congestion in the home Ring Peripheral Controller (RPC).

DRP7MSG2 The number of priority Level 2 messages discarded because of congestion in the home RPC.

DRP7MSG3 The number of priority Level 3 messages discarded because of congestion in the home RPC.

DRPEMSG1* The number of priority Level 1 Embedded Common Channel Interoffice Signaling 6 (ECIS6) messages discarded because of congestion in the home RPC.

DRPEMSG2* The number of priority Level 2 ECIS6 messages discarded because of congestion in the home RPC.

DRPEMSG3* The number of priority Level 3 ECIS6 messages discarded because of congestion in the home RPC.

ERSECTE The number of times the ERSEC count (that is, the number of 1 second intervals with at least one error) exceeded a threshold value.

GTTUNBC The number of global title messages received from, and destined to, the local network that failed translation because the destination is inaccessible.

GTTUNBT The number of global title messages received from, and destined to, the local network that had no translation assigned.

L7ACO The number of automatic changeovers on the link (near-end and far-end).

L7ACOTE The number of times the L7ACO count exceeded a threshold value.

L7BADRTG* The number of DCIS6 messages discarded in the incoming node because no translation data exists.

L7BOFR The number of received SS7 messages discarded due to a full receive buffer.

L7BOLR The number of times the receive buffer overloaded (no messages are discarded yet, but the far-end is informed).

L7BOLRT The duration of the L7BOLR.

L7FLD The number of times the link is declared failed, causing the link to be removed from service and diagnosed.

L7FLDT The duration of the L7FLD.

L7LCDIS1X The number of times transmit buffer occupancy reached the indicated threshold for Level 1 message discard. This count does not peg again until occupancy drops below the abatement threshold.

---

* The CCIS6 related measurements should always be zero (0).

L7LCON1X The number of times transmit buffer congestion occurs. This count is the number of times the transmit buffer occupancy reached the indicated threshold for congestion.

L7LCON1XT The duration of Level 1 congestion onset (ends at abatement). If the link is congested for 60 seconds or more, it may be taken out of service and diagnosed.

L7RTGAUD The number of times the automatic routing audit found an inconsistency in the point code routing data.

MSG7LOOP The number of messages discarded because they are "looping" in the network.

MSUDISC0 The number of Level 0 messages discarded because the link congestion level is 1 or higher.

MSUDISC1 The number of Level 1 messages discarded because the link congestion level is 2 or higher.

MSUDISC2 The number of Level 2 messages discarded because the link congestion level is 3.

SC7RERUA The number of received Signaling Connection Control Part (SCCP) messages destined for an unknown address (or global title).

SC7RERUATY The number of received SCCP messages destined for an unknown address (or global title) type.

SC7RERUNE The number of received SCCP messages destined for an unequipped subsystem.

SCRERPRO The number of locally originated SCCP messages destined for a prohibited subsystem.

SCRERUA The number of locally originated global title messages destined for an unknown address (that is, no global title translation found).

SCRERUATY The number of locally originated global title messages destined for an unknown address type (that is, an unassigned address type).

SCRERUNE The number of locally originated SCCP messages destined for an unequipped subsystem.

SPISP The number of times an adjacent signaling point is isolated because of local link failures.

SPISPT The duration of the Signaling Point Isolation (SPISP).

3. Signaling Network Performance Report, Part 2 (SNPR2)

3.01 The SNPR2 is a detailed report of signaling link performance. The report is automatically output once each hour. Data coverage should be 012/012 indicating twelve 5-minute periods (or 1 hour) of data are to be collected for the report. This report provides details on each signaling link in the office to allow troubleshooting of faulty links and the compilation of statistical data on each link.

3.02 This report and the 30MPR link exception report are the main sources of data for analysis of link failures and marginal performance. It provides an overview of the loss of signaling capability for the office according to link type and a detailed description of SS7 signaling link performance. It should be checked whenever signaling link problems are indicated.

3.03 The counts on this report are 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 to provide long term analysis of intermittent problems. When serious problems with specific links are identified, refer to Chapter 4, "Signaling Link Trouble."

3.04 Data is provided for each equipped link (as long as any measurement on the particular report line in question is nonzero). If there is no data available for a link, the type is shown as " *." The measurements for each link are listed on separate lines with link identification to the left of each (far-end CLLI code, layer number, link type, and group-member number). The basic layout of the report is shown in Figure 5-2.

Signaling Link Summary

3.05 This section of the report provides link totals for the office. Some of these totals may be zero, depending on the types of links equipped.

3.06 Measurements in this section are defined as follows:

L7AFLT	The duration of a link failure due to automatic action (that is, any reason other than manual removal)
L7MFLT	The duration of a link being manually out-of-service
L7PORT	The duration of far-end processor outage.

Loss of Signaling Capability

3.07 This section of the report indicates how often, and for how long, particular categories of links are unable to provide signaling. All CNI offices display counts for A-links. In STPs, separate counts are provided for B/D-links and C-links.

3.08 Measurements in this section are defined as follows:

CLFA	Cumulative total of all A-linkset failures in the office
CLFAT	The duration of the CLFA
EMRA	The number of emergency restarts on A-links, caused by the link failing while either the corresponding link at the mate office is Out-of-Service or all C-links are unavailable
EMRAT	The duration of the EMRA
SPIA	The number of times an adjacent signaling point is isolated because of a local A-link failure
SPIAT	The duration of the SPIA.

Signaling Link Performance

3.09 This section of the report provides the most important measurements for analyzing SS7 link performance. This includes counts of changeovers, errors, bytes retransmitted, failures and failure durations, discarded messages, congestions, and signaling point isolations.

3.10 Measurements in this section are defined as follows:

BYRX	The number of message signal unit octets retransmitted.
BYRXTE	The number of times the BYRX count exceeded a threshold value.
CLF	The number of linkset failures. A linkset failure is caused by the last available link in the set failing, possibly resulting in a signaling point isolation.
CLFT	The duration of the CLF (defined as the time between the last link in the set failing and any link in the set restoring).
CRCER	The number of data errors in received messages (specifically, failure of the cyclic redundancy check).
CRCERTE	The number of times the CRCER count exceeded a threshold value.
ERSEC	The number of 1-second intervals in which received messages had at least one error.

ERSECTE	The number of times the ERSEC count exceeded a threshold value.
L7ACO	The number of automatic changeovers on the link (near-end and far-end).
L7ACOTE	The number of times the L7ACO count exceeded a threshold value.
L7EMRPO	If there is ECIS6 signaling on the link, this is the number of emergency restarts caused by far-end processor outage. Otherwise, the count is always 0.
L7EMRPOT	The duration of the L7EMRPO.
L7EMR	If there is ECIS6 signaling on the link, this is the number of emergency restarts caused by local link failure. Otherwise, the count is always 0.
L7EMRT	The duration of the L7EMR.
L7FLD	The number of times the link is declared failed, causing the link to be removed from service and diagnosed.
L7FLDT	The duration of the L7FLD.
L7LCON1X	The number of times transmit buffer congestion is imminent, requiring messages to be discarded at the far-end.
L7LCON1XT	The duration of the L7LCON1X (if the link is congested for 60 seconds or more, it may be taken out of service and diagnosed).
L7POR	The number of times the far-end office began sending processor outage messages.
L7PORT	The duration of the far-end processor outage.
L7POX	The number of times that either the signaling link is not being serviced or the link node has failed and processor outage may be transmitted.
L7POXT	The duration of near-end processor outage (L7POX) in effect.
SPIPO	The number of times an adjacent signaling point is isolated because of a far-end processor outage.
SPIPOT	The duration of the SPIPO.
SPI	The number of times an adjacent signaling point is isolated because of a combination of a local failure and/or a received Transfer Restricted/Prohibited message.
SPIT	The duration of the SPI.

Report Output Format

```
xx REPT SMR ASNPR2HR STARTED

SIGNALING NETWORK PERFORMANCE REPORT - PART II

REPORTING OFFICE: local CLLI code          REPORT INTERVAL: daily
CURRENT GENERIC: gen_id                  AUTOMATIC REPORT
DATE: yy/mm/dd,  TIME: hh:mm:ss
REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
DATA COVERAGE: 012/012
                                        CCIS6    CCS7
QTOTAL NO. OF EQUIPPED LINKS:             0       nn
TOTAL LINK OOS TIME(SECS):                0        *
QDURATION RCV'D PROCESSOR OUTAGE:         0     L7PORT
QTOTAL NO. OF POOLS/LINKSETS:             0       nn

LOSS OF SIGNALING CAPABILITY ---
               ------EMR------
                PC       SEC
   A/E LINKS:    EMRA     EMRAT

   LOSS OF SIGNALING CAPABILITY ---
                 --CCS7 SPI--       --CCS7 LSF--
                PC       SEC       PC      SEC
   A/E LINKS:    SPIA     SPIAT     CLFA    CLFAT

  CCS7 SIGNALING LINK PERFORMANCE ---
                                ---ACO---     --ERSEC--     --CRCER--      -BYT-RXMT
FAR END CLLI-LAYER T GR-MEM    PC     TE     PC      TE     PC      TE     PC    TE
----------------  - ------ ------------ ------------ ------------ ------------
nnnn nn nn nnn-nn  a nn-nn L7ACO L7ACOTE ERSEC ERSECTE CRCER CRCERTE BYRX BYRXTE
nnnn nn nn nnn-nn  a nn-nn L7ACO L7ACOTE ERSEC ERSECTE CRCER CRCERTE BYRX BYRXTE

    *  Sum of L7AFLT and L7MFLT
```

Figure 5-2. Layout of the SNPR2 Report (Sheet 1 of 2)

```
CCS7 SIGNALING LINK PERFORMANCE ---
                                OOS-TIME  ----LSF---     --DCL-FLR-
FAR END CLLI-LAYER T CR-MEM    HH MM SS    PC    SEC       PC    SEC
 ------------------ - ------    --------  ----------     ----------
nnnn nn nn nnn-nn  a nn-nn     *     CLF    CLFI    L7FLD L7FLDI
nnnn nn nn nnn-nn  a nn-nn     *     CLF    CLFI    L7FLD L7FLDI
xx REPT SMR ASNPR2HR IN PROG

CCS7 SIGNALING LINK PERFORMANCE ---
                                 ---XMIT BUFFER---
                               MSURMV     CONG-LEV1       PRO-XMTD      PRO-RCVD
FAR END CLLI-LAYER T GR-MEM    PC      PC      SEC       PC    SEC     PC    SEC
------------------ - ------ ------ -------------- ------------ ------------
nnnn nn nn nnn-nn  a nn-nn     † L7LCON1X L7LCON1XT L7POX L7POXT L7POR L7PORT
nnnn nn nn nnn-nn  a nn-nn     † L7LCON1X L7LCON1XT L7POX L7POXT L7POR L7PORT


CCS7 SIGNALING LINK PERFORMANCE ---
                                --EMR--       --EMR-PO--     --SPI--    --SPI-PO--
FAR END CLLI LAYER T GR-MEM    PC    SEC     PC       SEC      PC SEC     PC    SEC
------------------ - ------ ------------ ---------------- -------- ------------
nnnn nn nn nnn-nn  a nn-nn  L7EMR L7EMRT L7EMRPO L7EMRPOT SPI SPIT SPIPO SPIPOT
nnnn nn nn nnn-nn  a nn-nn  L7EMR L7EMRT L7EMRPO L7EMRPOT SPI SPIT SPIPO SPIPOT

xx REPT SMR ASNPR2HR COMPL
    †  Sum of MSUDISC0, MSUDISC1, and MSUDISC2.
```

Figure 5-2. Layout of the SNPR2 Report (Sheet 2 of 2)

4. Machine Performance Report (MPR)

4.01 The MPR is a total office report that is output automatically for each hour and once for the entire day. The data coverage is 012/012 for the hourly report and 288/288 for the daily report. This report provides an overall view of the message switching capability for the office.

4.02 The report does not provide detailed measurements for each link or node. Instead, it shows cumulative counts for the entire office. This report can be used to determine the signaling status of the office in general (for example, the number of times it initialized and for how long no SS7 messages are processed) or the status of the CNI ring in general. Status information includes node Out-of-Service (OOS) counts, ring reconfigurations, and ring congestion levels.

4.03 This report should be checked daily for counts indicating ring node failures or degraded ring performance. The hourly reports from many periods should be compared for trends and abnormalities. A high count on one report is not necessarily an indication of problems. On the other hand, the same count(s) occurring at the same time each day may point to externally induced problems. If problems are indicated, the user should request detailed measurements of specific nodes with the **DUMP:SMEAS** input message.

NOTE:
For more details on the **DUMP:SMEAS** input message, refer to Chapter 6, "Displaying Signaling Measurements (**DUMP:SMEAS**)."

The basic layout of the report is shown in Figure 5-3.

System Initializations

4.04 This section of the report shows, for each subsystem, how many times specific system initialization levels occurred and for how long. An application initialization starts a CNI initialization, which starts an Interprocess Message Switch (IMS) initialization. Since initialization of each subsystem is triggered by a higher subsystem, the counts for a particular initialization level are normally the same for all subsystems.

4.05 Measurements in this section are defined as follows:

CINIT0 The number of Level 0 CNI initializations that started.

CINIT0T The duration of the CINIT0.

CINIT1 The number of Level 1 CNI initializations that started.

CINIT1T	The duration of the CINIT1.
CINIT3	The number of Level 3 CNI initializations that started.
CINIT3T	The duration of the CINIT3.
CINIT4	The number of Level 4 CNI initializations that started.
CINIT4T	The duration of the CINIT4.
INIT0	The number of Level 0 (audit level) IMS initializations. At this level, messages are being switched.
INIT0T	The duration of the INIT0, which does not include the time to boot.
INIT1A	The number of Level 1A (recovery level) IMS initializations. Tables are rebuilt and, although the CNI can switch messages, some may be lost.
INIT1AT	The duration of the INIT1A.
INIT1B	The number of Level 1B IMS initializations, during which no messages are switched.
INIT1BT	The duration of the INIT1B.
INIT3	The number of Level 3 IMS initializations. The CNI is booted, some nodes may be downloaded, and the ring may be quickly reconfigured.
INIT3T	The duration of the INIT3. This is exclusive of the time spent at Levels 0 and 1.
INIT4	The number of Level 4 (the highest level) IMS initializations. If successful, all ring nodes are downloaded and the ring restarted. If unsuccessful, either the CNI is aborted or diagnostics are run.
INIT4T	The duration of the INIT4.

No Message Signal Unit Processing

4.06 The peg count indicates how many times the CNI entered a state in which it could not process SS7 messages. This should be at least the sum of the IMS Levels 1B, 3, and 4, although the state could occur without an initialization. Measurements in this section are defined as follows:

NOCMG	The number of times processing of SS7 messages temporarily stopped
NOCMGT	The accumulated time during which no SS7 messages could be processed.

Ring Peripheral Controller Node Performance

4.07 This section of the report provides Out-of-Service counts and durations for Ring Peripheral Controller Nodes (RPCNs) in general, according to the major cause of

the change of state. There are three conditions that may cause this, which are all mutually exclusive in effect: automatic action, manual action, or the result of a ring reconfiguration.

4.08 Also provided is a cumulative count of the number of times any node restarted for any reason.

4.09 Measurements in this section are defined as follows:

OOSAU The number of times the node is automatically taken out-of-service or automatically made standby. This does not include cases where the node is an innocent victim of a ring reconfiguration, but does include cases where the ring is down.

OOSAUT The duration of the OOSAU.

OOSCFG The number of times the node is an innocent victim of a ring reconfiguration (it is then OOS or standby). This also includes cases where the ring is down.

OOSCFGT The duration of the OOSCFG.

OOSMN The number of times the node is manually made OOS or standby. This also includes cases where the ring is down.

OOSMNT The duration of the OOSMN.

RSTTRMT The number of times the node is restarted.

Link Node Performance

4.10 This section of the report provides out-of-service counts and durations for Link Nodes (LNs) in general, according to the major cause of the change of state. Also provided is a cumulative count of the number of times any node restarted for any reason.

4.11 Measurements in this section are defined as follows:

OOSAU The number of times the node is automatically taken out-of-service or automatically made standby. This does not include cases where the node is an innocent victim of a ring reconfiguration, but does include cases where the ring is down.

OOSAUT The duration of the OOSAU.

OOSCFG The number of times the node is an innocent victim of a ring reconfiguration (it is then OOS or standby). This also includes cases where the ring is down.

OOSCFGT The duration of the OOSCFG.

OOSMN The number of times the node is manually made OOS or standby. This also includes cases where the ring is down.

OOSMNT The duration of the OOSMN.

RSTTRMT The number of times the node is restarted.

Ring Performance

4.12 This section of the report provides a profile of ring performance during the reporting period, including counts and durations of automatic ring isolations, ring downtime, and manual ring isolations.

4.13 Measurements in this section are defined as follows:

MRNIAU The number of times the ring is automatically reconfigured with multiple isolated ring nodes

MRNIAUT The cumulative duration of ring configurations with multiple node isolations existing in the office due to automatic action

RDWN The number of times the entire ring is down

RDWNT The duration of the RDWN (if this is more than 1 second, a critical alarm is sounded)

RNIMN The number of times any ring nodes are isolated manually

RNIMNT The cumulative duration of ring configurations with isolated nodes existing in the office due to manual action

SRNIAU The number of times the ring is automatically reconfigured with one ring node isolated

SRNIAUT The cumulative duration of ring configurations with single node isolations existing in the office due to automatic action.

Internal Congestion

4.14 This section of the report indicates the general level of internal congestion in the CNI ring. An RPC count pegs each time any RPC node enters a particular level of ring receive buffer congestion. An LN count pegs each time any link node enters a particular level of ring receive buffer congestion.

4.15 The buffers become congested if IMS is delivering messages to the node faster than it is processing the messages already in the buffers. The congestion controls become progressively more severe as the occupancy level of the buffer increases. At RPC Level 1, LNs are warned of imminent overflow at their home RPC.

4.16 Measurements in this section are defined as follows:

RRBOVFLW1 The number of times the ring node's buffer has reached imminent overflow

RRBOVFLW2 The number of times the ring node's buffer is so full that non-IMS messages are discarded

RRBOVFLW3 The number of times the ring node's buffer is completely full (all messages are discarded).

Report Output Format

```
xx REPT SMR AMPRBR STARTED
MACHINE PERFORMANCE REPORT

REPORTING OFFICE: local CLLI code          REPORT INTERVAL: hourly or daily
CURRENT GENERIC: gen_id                  AUTOMATIC REPORT
DATE: yy/mm/dd,  TIME: hh:mm:ss
REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
DATA COVERAGE: 012/012

   SYSTEM INITIALIZATIONS

            LEVEL_0          LEVEL_1        LEVEL_1A        LEVEL_1B
          COUNT   SEC      COUNT   SEC    COUNT    SEC    COUNT    SEC
          -----------    -------------  -------------  -------------
   CNI   CINIT0 CINIT0T  CINIT1 CINIT1T       N/A             N/A
   IMS   INIT0  INIT0T        N/A        INIT1A INIT1AT   INIT1B INIT1BT

   SYSTEM INITIALIZATIONS

           LEVEL_3          LEVEL_4
         COUNT   SEC      COUNT   SEC
         -------------  -------------
   CNI   CINIT3 CINIT3T  CINIT4 CINIT4T
   IMS    INIT3  INIT3T   INIT4  INIT4T

   NO MESSAGE SIGNAL UNIT PROCESSING

      COUNT      SEC
    --------   -------
      NOCMG    NOCMGT

   RPC NODE PERFORMANCE - RPC COUNT: nn

    ERRORS        OOS_AUTO            OOS_MAN           OOS_CNFG
     COUNT    COUNT       SEC     COUNT      SEC     COUNT       SEC
    -------   ---------------     -------------     ---------------
    RSTTRMT   OOSAU    OOSAUT     OOSMN   OOSMNT     OOSCFG  OOSCFGT

   LN NODE PERFORMANCE - LN COUNT: nn

    ERRORS        OOS_AUTO           OOS_MAN           OOS_CNFG
     COUNT    COUNT       SEC   COUNT      SEC     COUNT       SEC
    -------   ---------------   -------------     ---------------
    RSTTRMT   OOSAU    OOSAUT   OOSMN   OOSMNT     OOSCFG  OOSCFGT
```

Figure 5-3. Layout of the MPR Report (Sheet 1 of 2)

```
RING PERFORMANCE

    SNGL ISOLAT      MULT ISOLAT     RING DOWN    MAN NODE ISOLAT
    COUNT    SEC     COUNT    SEC    COUNT SEC    COUNT        SEC
    -------------    -------------   ----------   ---------------
    SRNIAU SRNIAUT   MRNIAU MRNIAUT  RDWN RDWNT   RNIMN     RNIMNT


  INTERNAL CONGESTION
                                OVERFLOW     OVERFLOW     OVERFLOW
                                LEVEL_1      LEVEL_2      LEVEL_3
                                --------     --------     --------
  RPC RING RECEIVE BUFFER       RRBOVFLW1    RRBOVFLW2    RRBOVFLW3
   LN RING RECEIVE BUFFER         N/A        RRBOVFLW2    RRBOVFLW3

xx REPT SMR AMPRHR COMPL
```

Figure 5-3. Layout of the MPR Report (Sheet 2 of 2)

5. 15-Minute Marginal Performance Report (15MPR)

5.01 The 15MPR contains two types of Machine Resource Performance reports. The report is a combined office/detailed report. It describes:

- The performance of the operating system (APS)
- A detailed report of the CCS7 link nodes
- A detailed report on the DLN nodes.

If scheduled, the 15MPR report will be automatically output every 15 minutes

Header

5.02 This report should be checked to identify load sharing problems, and whenever link problems are suspected.

5.03 The basic layout of the report is shown in the example in Figure 5-4 for a 4ESS™ switch.

5.04 This section of the report provides office identification, report type, time, and date coverage.

3B Processor Real Time Usage

5.05 This section of the report provides a measure of the APS/3B real-time usage during the last 15 minutes. This section is applicable to the 1A ESS™ and 4ESS switches only.

5.06 Measurements in this section are defined as follows:

IDLE TIME (i1)	Percentage of 3B Processor real-time spent in an idle loop during the reporting interval
KERN TIME (i2)	Percentage of 3B Processor real-time spent in RTR kernal during the reporting interval
KPROC TIME (i3)	Percentage of time used in kernal processes during the reporting interval
USER TIME (i4)	Percentage of time used in user processes during the reporting interval
PAGES SWAPIN (i5)	Number of pages (2048 bytes) swapped in from disk during the reporting interval

PAGES SWAPOUT (i6) Number of pages (2048 bytes) swapped out to disk during the reporting interval

APS DKRATE (i7) Number of APS disk jobs per second

PROC CRTD (i8) Number of processes created during the reporting interval

PROC TERM (i9) Number of processes terminated during the reporting interval

CCS7 Link Node

5.07 This section of the report contains detailed performance data for each of the switch's CCS7 link nodes, by group and member.

CCS7 NODES (gp) Group Number

CCS7 NODES (mb) Member Number

BYTES IN (j1*) Number of incoming messages signaling unit bytes received at the processor

BYTES OUT (j2) Number of outcoming messages signaling unit bytes transmitted at the processor

MSUS IN (j3) Number of message signaling units received at the switch processor node

MSUS OUT (j4) Number of message signaling units transmitted out to network processor node

FLD CNT (j5) Failure count of message signaling unit messages between the SS7 switch and STPs.

* Refer to the example in Figure 5-4.

DLN Node

5.08 This section of the report provides detailed performance data for each of the DLN nodes, by group and member.

5.09 Measurement in this section are defined as follows:

DLN NODES (gp) Group Number

DLN NODES (mb) Member Number

BASE (j6) Number of base level cycles in DLN, during the reporting interval

TBSY (j7) Number of base levels whose duration is longer than 10 ms, occurring during the reporting interval

BLOCKS IN (j8)	Number of incoming signaling and non-signaling unit blocks to the switch
BLOCKS OUT (j9)	Number of outgoing signaling and non-signaling unit blocks from the switch to the network
MESGS IN (j10)	Number of incoming signaling messages to the switch, processed by the DLN
MESGS OUR (j11)	Number of outgoing signaling messages from the switch to the network, processed by the DLN
ERR IN (j12)	Number of incoming errors, including reformatting and translation errors
ERR OUT (j13)	Number of outgoing errors, including reformatting and translation errors.

NOTE:
This output message will vary among Lucent Technologies product lines. Refer to the input/output message manuals listed throughout this document and in Chapter 9.

```
RING REPT SMR A15MPR15            STARTED

MACHINE RESOURCE PERFORMANCE REPORT

REPORTING OFFICE: local clli code              REPORT INTERVAL: FIFTEEN MINUTES
CURRENT GENERIC: X INRT gen_id                 AUTOMATIC REPORT
DATE: yy/mm/dd,   TIME: hh:mm:ss
REPORT PERIOD (NWT): yy/mm/dd, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
DATA COVERAGE: 03/03

IDLE  KERN  KPROC  USER  PAGES    PAGES    APS      PROC  PROC
TIME  TIME  TIME   TIME  SWAPIN   SWAPOUT  DKRATE   CRTD  TERM
 i1    i2    i3     i4     i5       i6       i7       i8    i9

CCS7   BYTES   MSUS     FLD  DLN     BASE/  BLOCKS   MESGS    ERR
NODES  IN/OUT  IN/OUT   CNI  NODES   TBSY   IN/OUT   IN/OUT   IN/OUT
qp-mb    j1      j3      j5  qp-mb     j6     j8       j10      j12
         j2      j4                    j7     j9       j11      j13

RING SMR A15MPR15   COMPLETED
```

Figure 5-4. Layout of the 15MPR Report (4ESS™ Switch)

6. 30-Minute Marginal Performance Report (30MPR)

6.01 The 30MPR is a detailed exception report of signaling link performance. It could be output automatically each 30 minutes (data coverage is 006/006 indicating six 5-minute periods), but only if one of the measurements contained in the report exceeds some predefined threshold. This report identifies links that are showing marginal performance. The report provides a set of measurements that indicate various problems with the link, such as parity errors in received signaling units, alignment problems, excessive changeovers, or excessive downtime.

6.02 This report should be checked whenever link problems are indicated. The reports from many periods should be compared for trends and abnormalities. Look for failures associated with an individual link, with a group of links, or with a particular far-end office. When serious problems with specific links are identified, refer to signaling link maintenance procedures.

6.03 If any measurement in a particular part exceeds its threshold as specified in the **MOCT**, then all equipped links are printed in that part. Those measurements exceeding their thresholds are identified by an asterisk (*). If no measurements in a section exceed their thresholds, then that part is not printed. However, if the report is demanded with **OP:SMR** and no measurements in the report exceeded their thresholds, the message **NO MEASUREMENT EXCEPTIONS ENCOUNTERED** is output.

6.04 If there are exceptions to report, depending on how many links are included in the report, there may be many pages of output. The data is similar to that found in the SNPR2 report. The basic layout of the report is shown in Figure 5-5.

SS7 Links

6.05 This section of the report provides two groups of measurements. The first group contains the total OOS time, a count of Switching Units (SUs) received with parity errors, a count of bytes (octets) retransmitted, and the number of automatic changeovers initiated from the link. The second group contains the number of errored seconds and the percentage of total time the link is unavailable.

6.06 Measurements in this section are defined as follows:

BYRX	The number of message signal unit bytes (octets) retransmitted
CRCER	The number of data errors in received messages [specifically, failure of the Cyclic Redundancy Check (CRC)]
ERSEC	The number of 1-second intervals in which received messages had at least one CRC error

L7ACO The number of automatic changeovers on the link (near-end and far-end)

UNVL The percentage of time the link is unavailable.

SS7 Clusters

6.07 This section of the report shows peg counts and durations for each equipped cluster, both local and remote. The counts indicate that the office is unable to route messages to any destination in the indicated cluster. The corresponding linkset failure count also pegs when a route set becomes unavailable (see the SNPR1 report).

6.08 Measurements in this section are defined as follows:

RTESETUN The number of times any member of the cluster became inaccessible due to a linkset failure along the paths to the cluster (the set of routes to the cluster are unavailable)

RTESETUNT The total time during which any member in the cluster is inaccessible.

Report Output Format

```
xx REPT SMR A30MPR30 STARTED

SIGNALING LINK 30 MINUTE MARGINAL PERFORMANCE REPORT


REPORTING OFFICE: local clli            REPORT INTERVAL: half hourly
CURRENT GENERIC: gen_id                   AUTOMATIC REPORT
DATE: yy/mm/dd,  TIME: hh:mm:ss
REPORT PERIOD (NWT): yy/mm/dd, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
DATA COVERAGE: 006/006


  CCS7 LINKS:
                                      OOS TIM   CRCER      BY RX       AUTO
    FAR END CLLI-LAYER T GR-MEM      MIN  SEC                        CHG OVER
    ------------------ - ------     --------  -----     -------     --------
    nnnn nn nn nnn-nn  a nn-nn        †        CRCER      BYRX        L7ACO
    nnnn nn nn nnn-nn  a nn-nn        †        CRCER      BYRX        L7ACO


  CCS7 LINKS:
                                       ERSEC   UNVL
    FAR END CLLI-LAYER T GR-MEM
    ------------------ - ------      -----   ------
    nnnn nn nn nnn-nn  a nn-nn       ERSEC   UNVL
    nnnn nn nn nnn-nn  a nn-nn       ERSEC   UNVL

  CCS7 CLUSTERS:
                      ROUTE SET UNAVAILABLE
    CLUSTER    TYPE      COUNT        SEC
    -------    ------    ----------------------
      nn         nn      RTESETUN  RTESETUNI

xx REPT SMR A30MPR30 COMPL

† This is the sum of L7AFLT and L7MFLT.
```

Figure 5-5. Layout of the 30MPR Report

7. Link Engineering Report

7.01 This report is only output at the *A-I-Net* products STP. The Link Engineering Report is a detailed signaling link performance report that is automatically output every 15 minutes. The data coverage should be 003/003. This report provides detailed link utilization and exception data on each SLK in the office allowing users to determine loads and failure rates and generally compile statistical data. Due to the amount of data provided, there may be many pages of output.

7.02 This report is not intended for troubleshooting SLK problems. However, links that are known to carry traffic near capacity levels should be monitored during daily busy periods. The counts MSURECVD, MSUTRAN, OCTRECVD, and OCTTRAN (defined below) provide a good measure of traffic volume on the link. The basic layout of the report is shown in Figure 5-6.

SS7 Signaling Link Utilization Data

7.03 This section of the report shows those measurements indicating the operating conditions of the links (such as utilization and traffic levels).

7.04 Measurements in this section are defined as follows:

L7DIF	If data integrity flag indicates nonzero, the data collected is incomplete or invalid data measurement has been collected. If the data integrity flag indicates zero, the data collected is good.
L7RBFOC	Cumulative receive buffer length in bytes.
L7XBFLOOK	The number of transmit buffer visits by the link interface in order to calculate the average transmit and receive buffer lengths.
MSURECVD	The number of MSUs (Level 3 type data) received.
MSUTRAN	The number of MSUs transmitted.
OCTRECVD	The number of MSU octets received, not including flags between signal units.
OCTTRAN	The number of MSU octets transmitted.
Link Utilization	The UTIL field indicates the percentage of total link capacity being used. It is calculated as (8*T)/(C*L), where "T" is the larger of either octets received (OCTRECVD + MSURECVD) or octets transmitted (OCTTRAN + MSUTRAN), "C" is the link capacity in bps, and "L" is the length of the measurement period in seconds. For link engineering purposes, total traffic is calculated in octets per measuring period, with the MSU count added to account for one flag octet per message. Utilization should not typically exceed 40 percent for normal operation.

Signaling Link Exception Data

7.05 This section of the report shows those measurements indicating various problems with the link (such as congestion or link failure).

7.06 Measurements in this section are defined as follows:

DRLKINHB The duration of a link being manually Out-of-Service (user initiated)

ECCNGLV1 The number of times transmit buffer congestion is imminent, requiring messages to be discarded at the far-end

MSUDISC0 The number of Level 0 messages discarded because the link congestion Level is 1 or higher

MSUDISC1 The number of Level 1 messages discarded because the link congestion level is 2 or higher

MSUDISC2 The number of Level 2 messages discarded because the link congestion level is 3

TDCNGLV1 The duration of the ECCNGLV1

TDLSINAC The duration that a linkset is failed, beginning with the failure of the last link in the set and ending when any link in the set restores.

Report Output Format

```
xx STP REPT SMR SCLNKENG STARTED

CCS7 LINK ENGINEERING REPORT

REPORTING OFFICE: local clli            REPORT INTERVAL: 15 min
CURRENT GENERIC: gen_id                   AUTOMATIC REPORT
DATE: yy/mm/dd,  TIME: hh:mm:ss
REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
DATA COVERAGE: 003/003

   CCS7 SIGNALING LINK UTILIZATION DATA ---
                                DIF  UTIL      MSU BYTES        ROUTED MSGS
   LS FAR END CLLI-SLC T GR-MEM (HEX)         RCV       XMT     RCV         XMT
   -- ------------------------ ----- ---- ---------------- ----------------
   nn nnnnnnnnnnn-nn   a  nn-nn L7DIF  *   OCTRECVD OCTTRAN MSURECVD MSUTRAN
   nn nnnnnnnnnnn-nn   a  nn-nn L7DIF  *   OCTRECVD OCTTRAN MSURECVD MSUTRAN

   CCS7 SIGNALING LINK EXCEPTION DATA ---
                                CONGEST L1 SEC        FLR TIM         CLF     MSURMV
   LS FAR END CLLI-SLC T GR-MEM ONSET       DIS      AUTO     MAN       SEC       PC
   -- ------------------------ ----------------- ---------------- -------- ------
   nn nnnnnnnnnnn-nn   a  nn-nn ECCNGLV1 TDCNGLV1 DRLKFLT DRLKINHB TDLSINAC    **
   nn nnnnnnnnnnn-nn   a  nn-nn ECCNGLV1 TDCNGLV1 DRLKFLT DRLKINHB TDLSINAC    **

 xx STP REPT SMR SCLNKENG COMPL
```

*

This value is derived by the calculation explained in the text for "SS7 Signaling Link Utilization Data" in this chapter.

**

Equals MSUDISC0 + MSUDISC1 + MSUDISC2

Figure 5-6. Layout of the 15-Minute Link Engineering Report

8. 5-Minute Ring Exception Report (STPs Only)

8.01 This report is output only at *A-I-Net* products STPs.

8.02 This 5-minute Ring Exception Report (RINGEX) is a detailed exception report of RPC congestion status and is used in RPC engineering. It can be output automatically every 5 minutes (data coverage is 1/1), but only if one of the measurements contained in the report exceeds some predefined threshold. If the report is demanded through **OP:SMR** and if no measurements exceeded their thresholds, then the message **NO RPC OVERFLOWS ENCOUNTERED** is output.

8.03 This report identifies RPC nodes experiencing various levels of congestion. It should be used in conjunction with the MPR report to determine possible causes of the congestion and the appropriate actions to relieve it. Refer to the description of that report for more information. Give particular attention to overflow levels 2 and 3 (the RRBOVFLW2_ and RRBOVFLW3_counts).

NOTE:
Another measurement to look at that is a flexible format report is RPCBOF. This measurement pegs when the message switch tries to add a message to the RPC buffer when the buffer is full.

8.04 This is a one-page report with two parts (refer to Figure 5-7).

- Header — office identification (CLLI code and generic), report interval and type (automatic or demand), date and time, report period, and data coverage
- Details of the congestion status of each RPC's ring receive buffers (one node per line).

8.05 Congestion of the RPC ring receive buffers indicates that messages are being sent to the RPC from the ring faster than it can process those messages. The report shows peg counts for levels 0, 1, 2, and 3 and duration counts for levels 1, 2, and 3. All IUNs are notified of their home RPC's congestion status.

8.06 A few points to consider when interpreting the measurements are as follows:

- Level 0 is the normal no discard state. Messages are discarded at higher levels (only in IUNs, however).
- The peg count indicates how many times the buffer occupany reached the indicated level.

Figure 5-7 shows the ring exception report.

```
xx STP REPT SMR SCRINGEX STARTED
  RPC OVERFLOW REPORT

REPORTING OFFICE: local CLLI       REPORT INTERVAL: five minutes
CURRENT RELEASE: corel_id             AUTOMATIC REPORT
DATE: mm/dd/yy, TIME: hh:mm:ss
REPORT PERIOD (NWT): mm/dd/yy. hh:mm:ss     THRU mm/dd/yy. hh:mm:ss
DATA COVERAGE: NN/001

GRP    MEM        OVFLW LVL 0      OVFLW LVL 1       OVFLW LVL 2       OVFLW LVL 3
NUM    NUM          PC             PC     TIME       PC     TIME       PC     TIME
-----  -----  ---------------  ---------------  ---------------  ---------------
 nn     nn        RRBOVFLW0       RRBOVFLW1_        RRBOVFLW2_        RRBOVFLW3_
 nn     nn        RRBOVFLW0       RRBOVFLW1_        RRBOVFLW2_        RRBOVFLW3_

xx STP REPT SMR SCRINGEX COMPL
```

Figure 5-7. Layout of the RINGEX Report

9. Gateway Traffic Summary Report (STPs Only)

9.01 This report is output only at *A-I-Net* products STPs.

9.02 The Gateway Traffic Summary Report (GTSR) is a detailed report of SS7 gateway traffic performance. It includes internetwork and transport signaling load counts. SNM and SCCP Management messages, and Internetwork Global Title Translation (GTT) data. This report is output automatically each hour and day and on demand (data coverage is 288/288).

Header

9.03 This report provides office identification (CLLI Code and generic), report interval and type (automatic or demand), date and time, report period, and data coverage.

Internetwork Signaling Load Summary

9.04 The Internetwork Signaling Load Summary is indicaed by the number of octets (or bytes) received and transmitted and the number of messages (counted in MSUs) received and transmitted. These four counts together provide a good measure of the traffic flow on the links.

Transport Signaling Load Summary

9.05 The Transport Signaling Load Summary is similar to the Internetwork Signaling Load Summary, except that the messages are received from non-local networks and are not addressed to the local network. Also, messages are transmitted to non-local networks through an adjacent receiving network.

Internetwork Global Title Translation Summary

9.06 The Internetwork Global Title Translations Summary provides information about the failute and success of Global Title Translation (GTTs). The failures are indicated by blockage or congestion, no translation table, and no translation for address. The successes are indicated by messages from non-local networks.

SNM Messages Summary

9.07 Signaling Network Management (SNM) Messages are indicated by the following:

- Transfer Prohibited (TFP message signal units (MSUs)
- Transfer Restricted (TFR) MSUs
- Transfer Allowed (TFA) MSUs
- Signaling Route Set Test (SRST) MSUs
- Signaling Route Set Congestion Test (SRSCT) MSUs
- Signaling Link Test (SLT) MSUs
- Testing and Maintenance (T&M) MSUs
- Transfer Controlled (TFC) MSUs.

SCCP Management Messages Summary

9.08 The SCCP Management Messages Summary is indicated by Subsystem Allowed (SSA), Subsystem Prohibited (SSP), and Subsystem Status Test (SST) MSUs.

9.09 Figure 5-8 shows an example of the Gateway Traffic Summary report.

xx STP REPT SMR SCGTSR STARTED
GATEWAY TRAFFIC SUMMARY REPORT

REPORTING OFFICE: *local CCLI* *REPORT INTERVAL: hourly*
CURRENT RELEASE: *rel_id* AUTOMATIC REPORT
DATE: *mm/dd/yy*, TIME: *hh:mm:ss*
REPORT PERIOD (NWI): *mm/dd/yy, hh:mm:ss THRU mm/dd/yy, hh:mm:ss*
DATA COVERAGE: nnn/012

PAGE 1 OF z

xx STP REPT SMR SCGTSR IN PROG

---INTERNETWORK SIGNALING LOAD SUMMARY---

LINKSET	NID/ (CLU)*	OCTETS RCVD	OCTETS XMTD	MESSAGES RCVD	MESSAGES XMTD
LS1	NID1	OCTRECVD	OCTTRAN	MSURECVD	MSUTRAN
LS2	NID2	OCTRECVD	OCTTRAN	MSURECVD	MSUTRAN
:	:	:	:	:	:
LSj	NIDk	OCTRECVD	OCTTRAN	MSURECVD	MSUTRAN
LSj+1	NIDk	OCTRECVD	OCTTRAN	MSURECVD	MSUTRAN

PAGE 2 OF z

xx STP REPT SMR SCGTSR IN PROG

---TRANSPORT SIGNALING LOAD SUMMARY---

LS1	DESTNID1	OCTRCVNA	OCTTRNNA	MSURCVNA	MSURTNNA
:	:	:	:	:	:
:	DESTNIDk	:	:	:	:
LSj	:	OCTRCVNA	OCTTRNNA	MSURCVNA	MSUTRNNA

PAGE u OF z

* For a small network, the network identifier and cluster number fields must be included.

Figure 5-8. Layout of the GTSR Report (Sheet 1 of 3)

```
xx STP REPT SMR SCGTSR IN PROC

   ---INTERNETWORK GLOBAL TITLE TRANSLATION SUMMARY---
              GTT UNABLE GTT UNABLE  GTT UNABLE     GTT PERFD      GTT PERFD
   ORIGNID/   BLOCKG OR  NO TRNSLN    NO TRNSLN      MSGS FROM     RESULT DPC
    (CLU)*     CONGSTN      TABLE    FOR ADDRESS    NON-LOC NW     NON-LOC NW
   ------------------------------------------------------------------------------
   ORIGNID1   ZGTUNBIC   GTTUNTT      GTTUNADR       GTTPFDIC       GTTPFDPC

      :          :          :            :              :              :
   ORIGNIDK      :          :            :              :              :
      :          :          :            :              :              :
      :       ZGTUNBIC   GTTUNTT      GTTUNADR       GTTPFDIC       GTTPFDPC

   PAGE v OF z

   xx STP REPT SMR SCGTSR IN PROG

   ---SNM MESSAGES SUMMARY---

              RECEIVED SNM MESSAGES - SECTION 1
   LINKSET    TFP        TFR      TFA       SRST       SRSCT       STLT       T&M
             MSUs       MSUs     MSUs      MSUs        MSUs       MSUs       MSUs
   ------------------------------------------------------------------------------
   LS1    TFPRECD     TFRRECD   TFARECD   SRSTRECD   SRSCTRCD    SLTRECD    TSTMTRCD
    :        :           :         :          :          :          :          :
    :        :           :         :          :          :          :          :
   LSj    TFPRECD     TFRRECD   TFARECD   SRSTRECD   SRSCTRCD    SLTRECD    TSTMTRCD

   PAGE w OF z

              RECEIVED SNM MESSAGES - SECTION 2
   LINKSET     ORIGNID1      TFCGRECD
    :             :             :
    :          ORIGNIDk         :
    :             :             :
   LSj            :          TFCGRECD

   PAGE x OF z

              TRANSMITTED SNM MESSAGES
   LINKSET    TFP        TFR      TFA      TFC        SRST       SRSCT
             MSUs       MSUs     MSUs     MSUs       MSUs        MSUs
   ------------------------------------------------------------------------
     LS1   TFPTRAN    TFRTRAN   TFATRAN  TFCGTRAN   SRSTTRAN    SRSCTRAN
      :       :          :         :          :          :
      :       :          :         :          :          :
     LSj   TFPTRAN    TFRTRAN   TFATRAN  TFCGTRAN   SRSTTRAN    SRSCTRAN

   PAGE y of z

   xx STP REPT SMR SCGTSR IN PROG
```

Figure 5-8. Layout of the GTSR Report (Sheet 2 of 3)

```
xx STP REPT SMR SCGTSR IN PROG

   ---SCCP MANAGEMENT MESSAGES SUMMARY---

   LINKSET    SSA       SSA      SSP       SSP       SST       SST
              RCVD      XMTD     RCVD      XMTD      RCVD      XMTD
     LS1   SSARECD   SSATRAN  SSPRECD  SSPTRAN   SSTRECD  SSTTRAN
      :        :         :        :         :         :         :
      :        :         :        :         :         :         :
     LSj   SSARECD   SSATRAN  SSPRECD  SSPTRAN   SSTRECD   SSTTRN

   PAGE x OF z

   xx STP REPT SMR SCGTSR COMPL
```

Figure 5-8. Layout of the GTSR Report (Sheet 3 of 3)

NOTE:
All measurements represent peg counts.

10. Network Operations Report (STP Only)

10.01 This report is output only at *A-I-Net* products STPs.

10.02 The Network Operations Report is a detailed report of SS7 signaling link performance that is automatically output every 25 minutes. The data coverage should be 005/005 indicating five 5-minute periods (or 25 minutes) of data are to be collected. This report provides both summary and detailed exception data on each SLK in the office allowing users to determine the signaling condition of the SLKs and the network. Due to the amount of data provided, there may be many pages of output. The report is not intended for troubleshooting SLK problems.

10.03 The basic layout of the report is shown in Network Operations Report (Figure 5-9).

Signaling Load

10.04 This section of the report provides summary traffic data for all links in the office. These counts do include messages received in error.

10.05 Measurements in this section are defined as follows:

OCTRECVD The number of MSU octets received, not including flags between signal units

OCTTRAN The number of MSU octets transmitted

MSINVDPC The number of MSUs discarded due to a lack of routing data.

SS7 Signaling Link Exception Data

10.06 This section of the report provides data for each equipped link, as long as some measurement for that link exceeds its threshold.

10.07 Measurements in this section are defined as follows:

DRBSYDCL The duration of a receive buffer overload

DRLKFAIL The duration of a link being Out-of-Service due to automatic action, including the duration of declared failure

DRLKINHB The duration of a link being manually Out-of-Service (user initiated)

ECCNGLV1 The number of times transmit buffer congestion is imminent, requiring Level 0 messages to be discarded at the far-end

ECCNGLV2	The number of times transmit buffer congestion reached Level 2, requiring Level 1 messages to be discarded at the far-end
ECCNGLV3	The number of times transmit buffer congestion reached Level 3, requiring Level 2 messages to be discarded at the far-end
L7BOLR	The number of times the receive buffer overloaded (no messages are discarded yet, but the far-end is informed)
L7LCDIS1X	The number of times transmit buffer congestion caused queued messages to be discarded
L7POR	The number of times the far-end office began sending processor outage messages
LFNODISO	The number of times an adjacent signaling point is isolated because of a local failure or a received Transfer Restricted/Prohibited message
SPIPO	The number of times an adjacent signaling point is isolated because of a far-end processor outage
TDCNGLV1	The duration of the ECCNGLV1 (if the link is congested for 60 seconds or more, it may be taken out of service and diagnosed)
TDCNGLV2	The duration of the ECCNGLV2
TDCNGLV3	The duration of the ECCNGLV3
TNODEISO	The duration of the LFNODISO.

Report Output Format

```
xx STP REPT SMR SCNETOPR STARTED

NETWORK OPERATIONS REPORT

REPORTING OFFICE: glocal clli            REPORT INTERVAL: 5 minutes
CURRENT GENERIC: gen_id                   AUTOMATIC REPORT
DATE: yy/mm/dd,  TIME: hh:mm:ss
REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
DATA COVERAGE: 005/005

   SIGNALING LOAD ---        RECEIVED      TRANSMITTED
      CCS7 MSU BYTES:        OCTRECVD        OCTTRAN

   MSUS DISCARDED - ROUTING DATA ERROR       MSINVDPC

   CCS7 SIGNALING LINK EXCEPTION DATA ---
                                  FLD TIM            OVLD           POR
   FAR END CLLI-SLC T GR-MN   AUTO        MAN      PC        SEC     PC
   -------------------------  ----------------- ----------------  -----
   nnnnnnnnnnn-nn   a  nn-nn  DRLKFAIL DRLKINHB L7BOLR  DRBSYDCL  L7POR
   nnnnnnnnnnn-nn   a  nn-nn  DRLKFAIL DRLKINHB L7BOLR  DRBSYDCL  L7POR

   CCS7 SIGNALING LINK EXCEPTION DATA ---
                                     PI             CONG DIS L1
   FAR END CLLI-SLC T GR-MN      PC       PO       SEC        PC
   ------------------------- ------------------------  ---------
   nnnnnnnnnnn-nn   a  nn-nn  LFNODISO SPIPO TNODEISO  L7LCDIS1X
   nnnnnnnnnnn-nn   a  nn-nn  LFNODISO SPIPO TNODEISO  L7LCDIS1X

   CCS7 SIGNALING LINK EXCEPTION DATA ---
                                CONG ON L1         CONG ON L2         CONG ON L3
   FAR END CLLI-SLC T GR-MN    PC         SEC     PC         SEC     PC         SEC
   ------------------------- ----------------- ----------------- -----------------
   nnnnnnnnnnn-nn   a  nn-nn ECCNGLV1 TDCNGLV1 ECCNGLV2 TDCNGLV2 ECCNGLV3 TDCNGLV3
   nnnnnnnnnnn-nn   a  nn-nn ECCNGLV1 TDCNGLV1 ECCNGLV2 TDCNGLV2 ECCNGLV3 TDCNGLV3

xx STP REPT SMR SCNETOPR COMPL
```

Figure 5-9. Layout of the 5-Minute Network Operations Report

11. SS7 Feature Measurements

11.01 This part summarizes the measurements for the following SS7 features:

(a) Integrated Services Digital Network User Part (ISUP)

(b) Service Switching Point (SSP)/800

(c) Local Area Signaling Services (LASS)

(d) Network Interconnect (NI)

(e) Advanced Services Platform (ASP).

Integrated Services Digital Network User Part

11.02 Table 5-B provides a comparison of the ISUP feature traffic and plant measurements for the 1A ESS switch, 4ESS switch, and 5ESS switch.

Table 5-B. ISUP Traffic and Plant Measurements

Type	Measurement	1A ESS™ Switch TMC/EGO I PMxx	4ESS™ Switch MSC/OMC	5ESS® Switch Report/Section/Field
1	Incoming ISUP Call Attempts	159/007	5/1, 37/0	TRFC30/3/ISUPRQ
1	Outgoing ISUP Call Attempts	159/008	5/1, 37/0	TRFC30/3/ISUPOR
1	Incoming ISUP Messages	159/021-028		TRFC30/120/MSGIN
1	Outgoing ISUP Messages			TRFC30/120/MSGOUT
1	Tandem Calls Peg Count	159/042,043,044		PLANT/1A/TANDEM (count is not CCS7 specific)
1	Continuity Tone Decoder Peg Count Usage Overflow	 001/tg# 000/tg# 000/tg#	 02	 TRFC30/9/PEGCT TRFC30/9/TOTUSG TRFC30/9/OVFLOW
2 2 2	REL Sent w/ Circuit Group Congestion Switch Congestion Failures IMA-Backward Fail Message Originated	PM01	 11/4 11/4	 TRFC30/120/SWCONG PLANT/1B/INCOM-BACKWARD
2	IMA-Backward Fail Message Received			PLANT/1B/OUTGO-BKWDMSG
2	Abnormal Release Messages Sent During an ISUP Call Setup			TRFC30/120/ABNREL
2	REL Rec. w/ No Route to Destination Vacant Code	PM01		
2 2	REL Rec. w/ Circuit Group Congestion No Circuit Available Failures	PM01	 36/12	TRFC30/6/INCOM-BMFO TRFC30/120/NOCKT
2	REL Rec. w/ Switch Equipment Congestion	PM01*	11/4	
2	REL Rec. w/ Unallocated Number	PM01	11/4	TRFC30/120/BADNUM
2	REL Rec. w/ Temporary Failure	PM01	11/4	TRFC30/120/TMPFAIL
2	ACM Time-Out	PM01	25/3	PLANT/1B/OUTGO-TIMEOUTS
2	Address Incomplete Failures		36/0	TRFC30/120/ADDRINC
2	Busy Failures		FHC*	TRFC30/120/BUSY
2	Destination Out-of-Service		FHC	TRFC30/120/DESTOOS

* Reported via Final Handling Code (FHC)

Table 5-B. ISUP Traffic and Plant Measurements (Contd)

Type (Note)	Measurement	1A ESS™ Switch TMC/EGO I PMxx	4ESS™ Switch MSC/OMC	5ESS® Switch Report/Section/Field
2	ISUP Call Failure Any Other Reason		45/0	TRFC30/120/ISUP-OTHER
3	CCS7 IAM Not Processed	159/004		
3	Incoming Invalid Message Type	159/009	FHC	PLANT/3/INCOM-INVLDMSG
3	Unreasonable Message Received Out of Sequence Message on Call Setup		36/0	PLANT/3/INCOM-UNREASONABLE
3	Unreasonable Message Type Received		FHC	TRFC30/120/UNRMSG
3	CCS7 Attempts Encountering Signaling Faults	159/046	FHC	
3	Unsuccessful Call Attempts		NSPMP†	TRFC30/120/TOTAL UNSUCCESSFUL ATTEMPTS
3	Continuity Message Time-Out	PM01	36/0	
3	Trunk Rehunts Started Detected Glare	5/27	11/0	TRFC30/120/GLARE
3	Incoming Blocking Acknowledgment Signal Time-Out - Group Block Prev. Sent			PLANT/3/INCOM-ACKTO
4	Incoming Continuity Failure	PM01	36/0	PLANT/3/INCOM-COT
4	Outgoing Continuity Failure	PM01	36/0	
4	Trunk Rehunts Started - Unsatisfactory Response (COT)		36/0	TRFC30/120/COTFAIL
4	Trunk Rehunts Started - For Any Other Reason Not COT or Glare		NSPMP	TRFC30/120/OTHER

Note:

The type codes are:

1 = # ISUP Messages/Call Attempts
2 = # ISUP Release Messages
3 = # Abnormal Events
4 = # Maintenance Actions

Table 5-B. ISUP Traffic and Plant Measurements (Contd)

Type (Note)	Measurement	1A ESS™ Switch TMC/EGO I PMxx	4ESS™ Switch MSC/OMC	5ESS® Switch Report/Section/Field
4	Unequipped CIC Sent	PM01	36/6	
4	Unequipped CIC Received	PM01		
4	CCS7 Calls Cut Off in Stable State	PM01	MSR1‡	
4	Switch Cutoff Calls	PM01	MSR1	PLANT/1A/SWITCH
4	Blocked Messages Received Non-Group			TRFC30/120/BLKMSG
4	Blocking Signals Transmitted			PLANT/3/OUTGO-BLKXMT
4	Total Incoming MDIIs For All Signaling Types	PM01		PLANT/5/TOTAL INCOMING MDIIS
4	Total Outgoing MDIIs For All Signaling Types	PM01		PLANT/5/TOTAL OUTGOING MDIIS

Note:

The type codes are:

1 = # ISUP Messages/Call Attempts
2 = # ISUP Release Messages
3 = # Abnormal Events
4 = # Maintenance Actions

11.03 Additional information concerning the ISUP feature measurements can be found in the following documents: *1A ESS Switch, COEES Index 60*; *1A ESS Switch, OM-6A001 Output Message Manual*; *4ESS Switch, TG-4 Translation Guide*; and 235-070-100, *5ESS Switch Traffic and Plant Measurements*.

12. Service Switching Point/800

12.01 Table 5-C provides a comparison of the SSP/800 feature traffic measurements for the 1A ESS switch, 4ESS switch, and 5ESS switch.

12.02 Additional information concerning the SSP/800 feature measurements can be found in the following documents: *1A ESS Switch COEES Index 75, 4ESS Switch, TG-4 Translation Guide*, and 235-070-100, *5ESS Switch Traffic and Plant Measurements—Appendix 1.*

Table 5-C. SSP/800 Traffic Measurements

Count Type	1A ESS™ Switch TMC/EGO	4ESS™ Switch MSC/OMC	5ESS® Switch TRFC30, Sect 91
Total SSP/800 calls	164/000 or 165/001	6/0	NSC-800
Originated Number Service Calls	164/015	5/1	NSC-ORG
Received Number Service Calls	164/016	5/1	NSC-RCVD
ACG Blocked calls*	164/001 thru 164/004	49/0	NNMC-BLK-C
ACG control list overflows†	164/005 thru 164/010		
Failures before initial query	164/011	49/0	FAIL-CP-BIQ
Failures after initial query	164/012	49/0	FAIL-CP-AIQ
Abandons before seizure	164/013	49/0	ABDN-BS-OT
Abandons after seizure	164/014		ABDN-AS-OTBCA
Successful Service Control Point (SCP) queries	166/001	49/0	NSQ-800
Second Stage Failures			FAIL-2S-EA
Normal Response Message			NORM-RESP
Play Announcement Message			PLAY-ANNC

* The Automatic Call Gapping (ACG) was invoked because of excessive calling to vacant code or nonpurchased numbering plan area, SCP overload, mass calling, or Service Management System (SMS) initiation.

† There is an overflow count for each of six different ACG codes: 6-digit vacant, 10-digit vacant, nonpurchased numbering plan area, SCP overload, mass calling, and SMS initiated.

13. Local Area Signaling Services

13.01 Table 5-D provides a comparison of the LASS feature traffic measurements for the 1A ESS switch and 5ESS switch.

Table 5-D. LASS Traffic Measurements

Count Type	1A ESS™ Switch TMC/EGO	5ESS® Switch TRFC30, Sect 76
AR activations	148/030 and 148/032	AUTO RECALL-ACS
AC activations	148/031	AUTO CALLBK-ACS
AR deactivations	168/003 and 148/038	AUTO RECALL-CANC
AC deactivations	168/002	AUTO CALLBK-CANC
AR/AC immediate call setup	148/033	AUTO RECALL-ICS AUTO CALLBK-ICS
AR/AC time-out	148/037	AUTO RECALL-TO & AUTO CALLBK-TO
AR/AC busy after ringback	148/039	AUTO RECALL-BYRB & AUTO CALLBK-BYRB
AR overflow	148/040	AUTO RECALL-OVFL
AC overflow	168/000	AUTO CALLBK-OVFL
AR/AC long-term denial	148/041	AUTO RECALL-LTD & AUTO CALLBK-LTD
AR/AC short-term denial	148/042	AUTO RECALL-STD & AUTO CALLBK-STD
AR/AC delayed processing	148/034	
AR/AC number of ringbacks	138/035	
AR/AC number of ringbacks answered	148/036	
AR request block peg count	148/043	
AR request block usage count	148/044	
AC request block peg count	168/001	
AC request block usage count	168/004	
NOICLID customer's attempts	148/008	
COT activations	148/000	CUST ORIG TRACE-ACS
COT DN unavailable	148/001	CUST ORIG TRACE-UNAV
COT Denials	148/002	COT-DENIED

Table 5-D. LASS Traffic Measurements (Contd)

Count Type	1A ESS™ Switch TMC/EGO	5ESS® Switch TRFC30, Sect 76
Dialed DA access code DA ringing attempts	148/003 148/004	ACS (SDA) RING (SDA)
Dialed ICLID per-call privacy access code	148/005	PVACT
ICLID display deactivations	148/006	CNDDACT
ICLID display activations	148/007	CNDACT
Dialed SCF access code	148/026	ACS (SCF)
SCF calls forwarded	148/027	ATT (SCF)
Dialed SCR access code	148/028	ACS (SCR)
SCR calls rejected	148/029	MATCH (SCR)
Dialed SCA access code	174/000	ACS (SCA)
SCA calls allowed	174/001	ATT (SCA)
SCA calls refused	174/002	ANNC (SCA)
SCA calls rerouted	174/003	REROUTE (SCA)
Dialed CAR access code	174/004	ACS (CAR)
CAR calls allowed	174/005	ATT (CAR)
CAR calls refused	174/006	ANNC (CAR)
CAR calls rerouted	174/007	REROUTE (CAR)
Count Type	**1A ESS™ Switch TMC/EGO**	**5ESS® Switch TRFC30, Sect 72**
The total number of messages;; containing DNs that are sent to ISDN or analog station sets.	na*	DNMSGS
* *na* denotes "not applicable".		

NOTE:
The measurements include Inter-LATA calls as well as Intra-LATA usage.

13.02 Additional information concerning the LASS feature measurements can be found in the following documents: *1A ESS Switch, COEES Index 38*, 231-390-207, *1A ESS Switch Traffic Measurements Feature Document* or TG1A (1400 Series); and 235-070-100, *5ESS Switch Traffic and Plant Measurements*.

14. Network Interconnect

14.01 Table 5-E provide a comparison of the Network Interconnect (NI) feature traffic and plant measurements for the 1A ESS switch, 4ESS switch, and 5ESS switch.

Table 5-E. NI Traffic and Plant Measurements

Type	Measurement	1A ESS™ Switch TMC/EGO I PMxx	4ESS™ Switch MSC/OMC	5ESS® Switch Report/Section/Field
1	NI Call Attempts at the Originating EAEO Directly Connected to an IC/INC	170/000		
1	EA Call Attempts at the Originating EAEO Routed Direct Outgoing Call Attempts to an IC/INC	PM06	NSPMP*	PLANT/6/RDOUTG
1	EA Call Attempts at the Originating EAEO Routed Shared Outgoing Call Attempts to an IC/INC	PM06	NSPMP	PLANT/6/RTOUTG
1	NI Call Attempts at the Originating EAEO indirectly Connected to an IC/INC	170/001		
1	NI Call Attempts Entering the Originating LATA AT on CCS7 Trunk and Leaving the AT via a CCS7 Trunk to an IC/INC	170/002		
1	NI Call Attempts Entering the Originating LATA AT on an EAMF Trunk and Leaving the AT via a CCS7 Trunk to an IC/INC	170/003		
1	NI Call Attempts Entering the Originating LATA AT on a CCS7 Trunk and Leaving the AT via an EAMF Trunk to an IC/INC	170/004		
1	NI Call Attempts Incoming to the First Switch in the Terminating LATA	170/005		PLANT/6/DINC
1	EA Call Attempts Incoming to the First Switch in the Terminating LATA	PM06		PLANT/6/DINC
3	Time-Outs per IXC, while waiting for ACM directly connected at EAEO and AT	PM06		
3	Time-Outs per IXC, while waiting for CRA at AT	PM06		
3	Time-Outs per IXC, while waiting for SSD wink at AT during CCS7 to MF Interworking	PM06		

* Reported on the Network Switching Performance Measurement Plan (NSPMP)

Table 5-E. NI Traffic and Plant Measurements (Contd)

Type (Note)	Measurement TMC/EGO I PMxx	1A ESS™ Switch MSC/OMC	4ESS™ Switch Report/Section/Field	5ESS® Switch
3	Time-Outs per IXC, while waiting for Acknowledgment Wink at the AT for CCS7 to EAMF using Inter-LATA Signaling	PM06		
3	Time-Outs per IXC, while waiting for Acknowledgment Wink at the AT for CCS7 to EAMF using International Signaling	PM06		
3	Call Attempt Failures due to Unreasonable Messages Received, per IXC, while waiting for First Backward Message	PM06		
3	Incoming CCS7 MDII			PLANT/6/I7MDII
3	Direct Incoming MDII	PM06		PLANT/6/DINMDII
3	Outgoing CCS7 MDII			PLANT/6/O7MDII
3	Direct Outgoing MDII	PM06		PLANT/6/DOTMDII
4	Call Failures due to CCS7 Continuity Failures per IXC - EAEO to IXC	PM06		
4	Call Failures due to CCS7 Continuity Failures per IXC - AT to IXC	PM06		
4	CCS7 Continuity Failures - Per Carrier		NSPMP	PLANT/6/COTFAIL
4	Number of Non-Priority 1 IAMs Received Per IXC	PM06		

Note:
The type codes are:

1 = # ISUP Messages/Call Attempts
2 = # ISUP Release Messages
3 = # Abnormal Events
4 = # Maintenance Actions.

14.02 Additional information concerning the NI feature measurements can be found in the following documents: *1A ESS Switch, COEES Index 90*, and 235-070-100, *5ESS Switch Traffic and Plant Measurements*.

15. Advanced Services Platform

15.01 Advanced Service Platform (ASP) traffic measurements can be separated into two categories: Service Switching Point (SSP) related measurements and Network Access Point (NAP) related measurements.

15.02 The following documents can be referenced for more information about the ASP traffic measurements: 235-190-125, *5ESS Switch Advanced Services Platform Feature Document*; 235-070-100, *5ESS Switch Traffic and Plant Measurements— Appendix 1*; 231-390-520, *1A ESS Switch Advanced Services Platform, Network Access Point Feature*; *231-390-519, 1A ESS switch Advanced Services Platform/Service Switching Point (ASP/SSP) Feature Document;1A ESS Switch, COEES Index 91; TG-4 Translation Guide, 4ESS Switch*; and *234-090-019, 4ESS Switch— Advanced Intelligent Network (AIN) Users' Guide.*

ASP SSP Traffic Measurements

15.03 Table 5-F lists the 1A ESS switch ASP/SSP traffic measurements.

Table 5-F. 1A ESS™ ASP/SSP Traffic Measurements

Measurement	1A ESS® Switch	
	TMC	EGO
Signaling Failure - Time-Out at SSP count	180	000
Invalid Command Message count	180	001
Return Error or Reject Message count	180	002
Abandon Before Outpulsing count	180	003
No Trunks Available for Publicor Autonomous Routing count	180	004
All Private Routes Busy count	180	005
ASP Calls Originating in SSP—Dialing Complete count	180	006
ASP Queries Sent to the SCP count	180	007
Normal Route Response Message Received count	180	008
Call Processing Failure Before Initial Query count	180	009
Call Processing Failure After Initial Query count	180	010
Resource Unavailable Before Initial Query count	180	011
Non-Fatal Resources Unavailable count	180	012
ASP Calls Received From Another Switch count	180	013
Play and Collect Messages From the SCP count	180	014
Play Announcement Messages from the SCP count	180	015
ASP Attempts to Access Announcement Circuit count	180	016
ASP Attempts Failed to Access Announcement Circuit count	180	017
Serial Triggering Overflow count	180	018
Termination Notification Requests Received by the SSP count	180	019
Termination Notification Responses count	180	020
Invalid Command Sequence count	180	021
Resource Unavailable After Initial Query count	180	022
Network Management (NM) Control Blocks count	180	023
ASP/SSP Calls Blocked by SCP Overload Control count	180	024
ASP/SSP Calls Blocked by SMS Control count	180	025
ASP/SSP SCP Overload Control Not Accepted Due to Control Block Being Full count	180	026
ASP/SSP SMS Control Not Accepted Due to Control Block Being Full count	180	027

Table 5-F. 1A ESS™ ASP/SSP Traffic Measurements (Contd)

Measurement	1A ESS™	
	TMC	EGO
Termination Notification Register Usage count	180	028
Termination Notification Register Usage count	180	029
Termination Notification Register Peg count	180	030
Termination Notification Register Overflow count	180	031
ASP/SSP Message Block Usage count	180	032
ASP/SSP Message Block Up/Down count	180	033
ASP/SSP Message Block Peg count	180	034
ASP/SSP Message Block Overflow count	180	035
Reserved for future ASP/SSP Use	180	036-050

NOTE:

There are several types of error checks during initial processing of incoming Transaction Capabilities Application Part (TCAP) messages, before it is known whether the message is an ASP message or an SSP/800 message. These errors are included in existing general number service measurements that appear on Section 91 of the 5ESS Switch TRFC30 report.

Tools

6

Contents Page

Contents Page

Contents Page

Contents

Page

Contents

Contents Page

Contents Page

Tools

6

1. Introduction

1.01 The tools described in this section are intended to ensure consistency of Signaling System 7 (SS7) related data between signaling points. Table 6-A summarizes the input commands needed to manually initiate each test.

1.02 For a detailed explanation of format of each input message, refer to the following input manuals:

- IM-6A001, *1A ESS Switch Input Message Manual*
- IM-6A002, *1A ESS Switch/APS Input Message Manual*
- IM-4A000, *4ESS Switch Input Message Manual*
- IM-4B000, *4ESS Switch Input Message Manual*
- IM-4A001, *4ESS Switch/APS Input Message Manual*
- IM-4B001, *4ESS Switch/APS Input Message Manual*
- 235-600-700, *5ESS Switch Input Message Manual*
- 270-750-404, *A-I-Net* STP *Input Message Manual* (Release 2)

Table 6-A. Summary of Tools to Verify Data Consistency

Tool Name	1A ESS™ Switch	4ESS™ Switch	5ESS® Switch	*A-I-Net*® STP	*A-I-Net* SCP
CIRCUIT QUERY	TQ-TNN TQ-GROUP TQ-DPC TQ-ABORT TQ-ALL TQ-STOP TQ-RESUME	TEST:TRK,CIN;TQU	AUD:CCSTQ,TKGMN	*na**	*na**
CIRCUIT VALIDATION	T-TNN-CV TRK-GROUP-CV	TEST:TRK,CIN;TIC	AUD:CCSXLATE, TKGMN	*na**	*na**
SLK DATA	OP:SLK	OP:SLK	OP:SLK	OP:SLK	OP:SLK
SLK MONITOR	MON:SLK	MON:SLK	MON:SLK	MON:SLK	OP:LSST
SIGNALING MEASUREMENTS	DUMP:SMEAS	DUMP:SMEAS	DUMP:SMEAS	DUMP:SMEAS	DUMP:MEAS
ROUTING DATA	OP:C7NET	OP:C7NET	OP:C7NET	OP:C7NET	OP:RS†
MRVT TEST	EXC:MRVT CHG:MRVT	EXC:MRVT CHG:MRVT	EXC:MRVT CHG:MRVT	EXC:MRVT CHG:MRVT	*na**
SRVT TEST	EXC:SRVT CHG:SRVT OP:TPC;TYPE	EXC:SRVT CHG:SRVT OP:TPC;TYPE	EXC:SRVT CHG:SRVT OP:TPC;TYPE	EXC:SRVT CHG:SRVT OP:TPC;TYPE	*na** *na**
MESSAGE TRAP	SET:TRAP ALW:TRAP INH:TRAP STOP:TRAP OP:TRAP	SET:TRAP ALW:TRAP INH:TRAP STOP:TRAP OP:TRAP	SET:TRAP ALW:TRAP INH:TRAP STOP:TRAP OP:TRAP	SET:TRAP ALW:TRAP INH:TRAP STOP:TRAP OP:TRAP	SET:TRAP ALW:TRAP INH:TRAP STOP:TRAP OP:TRAP
SSP/800 QUERY	SSP-EIGHT	TEST:DSIG;NS800	TST:NS800	*na**	*na**
LASS SCREEN LIST EDITING VALIDATION	OP:LASSRQST	*na**	OP:LASSRQST	*na**	*na**
ASP TEST QUERY	TEST:ASP‡	TEST:TCAPAIN‡	TST:ASP‡ TST:ASPTQ‡	*na**	*na**
OSPS CREDIT CARD	*na**	*na**	TST:CCRD	*na**	*na**
SEND PT2 MESSAGE TO SEAS	*na**	*na**	*na**	*na**	TST:SEAS PT2

* *na* denotes "not available"

† Point Code.

‡ Refer to Part 13 for specific references.

2. Circuit Query Test

2.01 This test verifies the consistency of the call processing trunk states and trunk maintenance states at both ends of an SS7 trunk. State consistency does not imply that the states at both ends are identical. There are several valid state combinations. The circuit query test checks the states at the two ends of the trunk, and if an unacceptable combination exists (that is, an inconsistent state), corrective action is taken by the switch that initiated the query. The intent of the corrective action is to put both ends of the circuit into one of the 13 valid state combinations shown in Tables 6-B, 6-C, and 6-D.

Table 6-B. Valid Call Processing (Busy/Idle) Trunk State Combinations (Note)

Near-End	Far-End
IDLE	IDLE
ICC BUSY	OGC BUSY
OGC BUSY	ICC BUSY
* ICC means Incoming Circuit and OGC means Outgoing Circuit.	

Table 6-C. Valid Trunk Maintenance (Blocking) State

Near-End	Far-End
ACTIVE	ACTIVE
LOCALLY AND REMOTELY BLOCKED	LOCALLY AND REMOTELY BLOCKED
LOCALLY BLOCKED	REMOTELY BLOCKED
REMOTELY BLOCKED	LOCALLY BLOCKED

Table 6-D. Transient and Unequipped States

Near-End	Far-End
TRANSIENT	TRANSIENT
TRANSIENT	UNEQUIPPED
TRANSIENT	OTHER
UNEQUIPPED	TRANSIENT
UNEQUIPPED	UNEQUIPPED
OTHER	TRANSIENT

Manual/Automatic Operation

2.02 To manually initiate the test, refer to Table 6-A for input messages associated with each switch type.

2.03 Each switch type executes the circuit query test on an automatic basis. As shown in Table 6-E, however, the schedule and extent of the testing vary by switch type.

Table 6-E. Automatic Execution of Circuit Query Test by Switch

1A ESS™ Switch	4ESS™ Switch	5ESS® Switch
The whole office is queried once between 8 p.m. and 6 a.m.	The whole office is routinely queried up to several times per day as a function of office size, the number of trunks, and the available real time (Audit 95). One trunk in each trunk subgroup is routinely queried at a much higher rate than Audit 95. Completion rate is a function of the office size, the number of trunks, and the available real time (Audit 96).	The whole office is queried routinely (approximately once per day). The interval between queries is determined by the "**TRK QRY**" value in Office Parameters, RC View 8.15.

Example of Operation

2.04 Assume that the near-end switch initiates a circuit query test on a trunk, the near-end is remotely blocked, and the far-end is locally and remotely blocked.

NOTE:
The near-end state is caused by the far-end originating a blocking message to the near-end.

2.05 Since this is an invalid trunk maintenance state combination, the circuit query test results in corrective action being taken. The near-end switch sends an unblocking message to the far-end, resulting in a valid maintenance state combination (that is, the near-end remotely blocked and the far-end locally blocked).

Special Considerations

2.06 The 1A ESS™ switch provides the capability to turn circuit query testing on or off to a connecting switch. Refer to the **RC:POINTC** input message (**CQA** keyword) in 231-318-334, *Trunk Translation Recent Change Formats* for more detail.

NOTE:
It is recommended that circuit query be allowed for all connecting switches.

2.07 The 4 ESS™ switch provides the capability to turn the circuit query test off by inhibiting audits 95 and 96 using the **INH:AUD** input message. If these audits have been inhibited, they can be reactivated using the **ALW:AUD** input message.

NOTE:
It is recommended that audits 95 and 96 be allowed at all times.

2.08 The 5ESS® switch provides the capability to turn circuit query testing on/off throughout the whole office or on a trunk group basis. If the need arises to inhibit the test throughout the 5ESS switch, input message **INH:CCSTQ** can be used. One can subsequently allow the office-wide inhibited test using input message **ALW:CCSTQ**. If office-wide testing is allowed, the circuit query test can be inhibited on a trunk group basis using RC View 5.1 (**TRK QUERY** field). Refer to 235-118-222, *5ESS Switch Recent Change Menu Mode/Text Interface*, and 235-600-700, *5ESS Switch Input Manual*, for more detail.

NOTE:
It is recommended that Circuit Query be allowed throughout the switch at all times.

3. Circuit Validation Test

3.01 The Circuit Validation Test (CVT) is used to ensure that connecting switches have sufficient and consistent translation data in order to place a call on a specific circuit. The test provides informational results only; no automatic corrective action is taken as a result of executing the test and call processing is unaffected on either switch. The test must be manually initiated (refer to Table 6-A).

Specifically, the test checks six characteristics of the trunk facility:

(1) Trunk Circuit Identification Code Assignment

The test validates whether or not connecting switches have an assigned Trunk Circuit Identification Code (TCIC) value.

(2) *Common Language** CLLI code/Circuit Identification Number

If far-end Circuit Identification Number information or the CLLI code is returned, it is checked for consistency.

NOTE:
The 1A ESS switch does not keep record of far-end CLLI code nor does it check this information. The 5ESS switch performs this test if the CLLI code is provided in the CVT. The 4ESS switch keeps a record of all far-end CLLI codes and checks the CLLI if it is returned.

(3) Glare Control

This validates that the glare control specified at each end of a two-way trunk group is complementary. The rules available are:

Odd/Even Using this rule, even trunk circuit identification codes should be controlled by the switch with the higher point code; odd trunk circuit identification codes should be controlled by the switch with the lower point code. The test only checks that glare control is not specified in such a way that there would be a conflict. It does not verify hunt direction.

All/None Using this rule, one switch controls all trunk circuit identification codes, the other switch controls none. There is no recommendation on which end should be all or none. However, each end must agree with the other.

(4) Circuit Group Carrier Indication

Information is provided, if known, on the circuit group. The information indicates whether the circuit group contains analog and/or digital trunks.

---

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

(5) Carrier Alarm Indicator

Information is provided, if known, on the type of alarming used. The information indicates whether the alarming is software-based or hardware-based. Inconsistent use of alarming can impact treatment of calls; in some cases, it can tear down calls.

(6) Continuity Check Requirements Indicator

If known, information is provided concerning the Voice Path Assurance (VPA) data. The information indicates how the voice circuit is set up for VPA.

3.02 An area that can indicate call processing failure is the Circuit Group Characteristics Indicator Parameter checks. Table 6-F describes the test, the test results, and potential sources of failure.

Table 6-F. Circuit Group Characteristics Indicator Parameter Check

Item	OK to Fail	Possible Cause
Double Seizing Control Indicator (Glare)	No	Incorrect population of office data via Recent Change (RC).
Circuit Group Carrier Indicator	Yes	Some Lucent Technologies switches do not have this data available. Always encoded UNKNOWN.
Carrier Alarm Indicator	Yes	No rules that require it to agree. Could indicate RC input problem.
Continuity Check Requirement Indicator	Yes	Lucent Technologies codes as UNKNOWN for consistency.

3.03 If the double seizing indicator (Glare) test fails, verify that the setting is correct at each end of the circuit. Then verify that the trunk hunt direction is correct for two-way trunks. Failure to do so may affect call processing.

Special Considerations

3.04 Each switch uses different terms to identify the validation test. The 1A ESS switch uses the term CVT, the 5ESS switch uses the term Translations Test, and the 4ESS switch uses the term Trunk Integrity Check.

One-Way Trunk Groups

3.05 TR-NWT-000246 provides the rules for the test on 1-way trunk groups. The rule is that the outgoing trunk controls ALL circuits and incoming trunk controls NONE. This rule is not enforced by recent change procedures. The test passes or fails depending on trunk data defining it as 1-way incoming or 1-way outgoing.

3.06 If a CVT test fails on a 1-way trunk group, it must be determined if the failure is due to:

(1) A 1-way/2-way mismatch

(2) A wrong definition of directionality on one end or the other

(3) One end of the trunk not recognizing the new CVT rule per the TR-NWT-000246 contribution.

Try to correct the situation based on information output on the Receive-Only Printer (ROP) at the failing switch. If the test cannot pass and verification of the translation data indicates it should pass, accept the failure and report it to technical assistance personnel, particularly for the last case.

3.07 In all cases, a test failure is not fatal and does not impact call processing capabilities.

4. Displaying Signaling Link Data (OP:SLK)

4.01 The **OP:SLK** input message is used to provide status information for one or more SS7 signaling links. Refer to the appropriate Input Message/Output Message (IM/OM) manuals (shown in Chapter 9, "References") for the proper format of the **OP:SLK** input and output messages.

4.02 This tool gives a printout of various link data elements, depending on the options specified in the input request. Some options currently available are:

(a) A detailed report including signaling link abnormal conditions (**ABNORMAL** keyword)

(b) A detailed report including signaling link configuration data (**FIX** keyword)

(c) A detailed report including some routing information (**ROUTING** keyword)

(d) A detailed report of the dynamic signaling link information (**RAW** keyword).

Example of Operation

4.03 This tool has also proven helpful in establishing the state (for example, growth, 1-way incoming only, 1-way outgoing only, or 2-way normal) of any equipped Direct Link Nodes (DLNs) in the switch.

4.04 Execution of this tool is invoked by the **OP:SLK** input message. Sample output shown in Figure 6-1 was generated using an **OP:SLK(32,3)** input message on a 1A ESS switch.

```
        OP SLK 32 3 IN PROG
CST MON JUN 24 08:52:30:081 1991
SLK 32 03   FISHINGTIME  AVL  IS
CST MON JUN 24 08:52:30:191 1991

        OP SLK 32 3 COMPL
```

Figure 6-1. OP:SLK ROP Printout

4.05 The output message indicates that the signaling link connected to link node (32,3) is available and in-service. The far-end of the Signaling Link (SLK) has a CLLI code of "FISHINGTIME."

5. Monitoring the Signaling Links (MON:SLK)

5.01 Signaling link (SLK) monitoring should be performed when a switch or new SLK is being "linked up" to an SS7 network, and verification that the SLK is operational and is needed. The SLK monitoring should be performed at the switch (near-end) and at the Signaling Transfer Point (STP) "far-end" of the signaling link.

5.02 During preservice testing, the SLK monitor provides valuable link data about incoming SS7 protocol Levels 2 and 3 signaling messages. Because the SLK is placed in the "unavailable" (UNAV) test state to do preservice testing, no alarms are generated nor does the SLK interact with the network.

5.03 The output from SLK monitoring is also helpful when an SLK cannot be made active. Signaling link activation trouble is evident when one (or more) of the following conditions occur:

(a) Connectivity between the STP and switch cannot be established.

(b) Prove-in fails.

(c) Prove-in is successful, but a Signaling Link Test (SLT) is not acknowledged.

5.04 Refer to Table 6-A for the appropriate input message to use for Lucent Technologies products. Refer to the appropriate IM/OM manuals ("Introduction" in this chapter) for the proper format of the **MON:SLK** input and output messages.

Sample Outputs

5.05 The SLK monitoring provides an indication of which condition has occurred, so that subsequent troubleshooting can take place. Sample outputs of **MON:SLK** are summarized in Table 6-G.

Table 6-G. MON:SLK Output Summary

Signaling Link Trouble	MON:SLK Output
No Signaling Link Connectivity between the switch and the STP	**ALIGNMENT NOT POSSIBLE, T2 EXPIRED**
Prove-In Fails	**ALIGNMENT NOT POSSIBLE, T2 EXPIRED** **ALIGNMENT ERROR RATE THRESHOLD EXCEEDED**
Prove-In Successful But SLT Acknowledgment Time-Out	**ALIGNMENT NOT POSSIBLE, T2 EXPIRED** **PROVE-IN QUEUED** **CCS7 SLT** **CCS7 SLTA TIMER EXPIRED**
Prove-in Successful But SLT Is Not Acknowledged	**ALIGNMENT NOT POSSIBLE, T2 EXPIRED** **PROVE-IN QUEUED** **PROVE-IN COMPLETE** **CCS& SLT** **CCS7 SLT - NOT ACKED**

5.06 In addition, SLK monitoring is useful as a general troubleshooting tool. It can be used to identify incoming signaling network management messages [for example, Transfer Restricted (TFR), Changeover Requests, Acknowledgement Time-Outs, etc.].

5.07 An example output message can be found in "Link and Facility Activation Procedures" in Chapter 2.

6. Displaying Signaling Measurements (DUMP:SMEAS)

6.01 The **DUMP:SMEAS** input message is used to provide a listing of the SS7 signaling measurements from switch history files. Refer to the appropriate IM/OM manuals ("Introduction") for the proper format of the **DUMP:SMEAS** input and output messages.

6.02 This tool gives a raw dump of the measurements for one or more signaling links, depending on the history file specified in the input request. The following history files are currently available:

(a) Current 30-minute data file

(b) Current hour data file

(c) Current day data file

(d) Last 15-minute data file

(e) Last 30-minute data file

(f) Last hour data file

(g) Last day data file

(h) Last period measurement structure.

Sample Output

6.03 Execution of this tool is invoked by the **DUMP:SMEAS** input message. A sample of possible Common Network Interface (CNI) and Interprocess Message Switch (IMS) measurements for **DUMP:SMEAS** is shown in Tables 6-H and 6-I.

Table 6-H. Valid CNI Measurement IDS

Measurement	Description
BYMSUR (CCS7)	Message signal unit bytes received.
BYMSUX (CCS7)	Message signal unit bytes transmitted.
BYR (CCS7)	Total bytes received excluding flags.
BYRX (CCS7)	Retransmitted bytes including flags.
BYRXTE (CCS7)	Threshold exceeded for BYRX.
BYSR (CCS7)	Non-Embedded Common Channel Interoffice Signaling 6 (ECIS6) bytes received, excluding flags.
BYSX (CCS7)	Non-ECIS6 bytes transmitted.
BYX (CCS7)	Total bytes transmitted excluding flags.
CLF (linkset)	Linkset failure.
CLFA (Office)	A-linkset failure.
CLFAT (Office)	Duration of A-linkset failure.
CLFSP (Office)	Linkset failure.
CLFSPT (Office)	Duration of linkset failure.
COS7CRFSRCM (CCS7)	Number of times a CREF message is sent due to a source match.
COS7DCHNOOS (CCS7)	Number of times an incoming CO-SCCP message is discarded due to destination D-channel being out-of-service.
COS7DSDSRCM (CCS7)	Number of times a CO-SCCP message is discarded due to source match.
COS7ERRSRCM (CCS7)	Number of times an ERROR message is sent due to a source match.
COS7LCNINV (CCS7)	Number of times an incoming CO-SCCP message is discarded due to an invalid or unequipped LACID.
COS7RLCSRCM (CCS7)	Number of times an RLC message is sent due to source match.
CRCER (CCS7)	Cyclic redundancy check errors.
CRCERTE (CCS7)	Threshold exceeded for CRCER.
DDCLFLABN (CCS7)	Cumulative duration of SLK declared failures due to abnormal condition.
DDFLHWP (CCS7)	Cumulative duration of SLK declared failures due to general hardware problems.
DDCFLSWP (CCS7)	Cumulative duration of SLK declared failures due to general software problems.
DDCFLXDA (CCS7)	Cumulative duration of SLK declared failures due to excessive delay of acknowledgment.
DDCFLDC (CCS7)	Cumulative duration of SLK declared failures due to excessive congestion durations.
DDCFLXER (CCS7)	Cumulative duration of SLK declared failures due to excessive error rate.
DRLNKUNV (CCS7)	Total duration of link unavailability for user traffic.
DRP7MSG1 (CCS7)	Number of priority Level 1 messages dropped due to Ring Peripheral Controller (RPC) congestion.
DRP7MSG2 (CCS7)	Number of priority Level 2 messages dropped due to RPC congestion.
DRP7MSG3 (CCS7)	Number of priority Level 3 messages dropped due to RPC congestion.
DRPEMSG1 (CCS7)	Number of priority Level 1 ECIS6 messages dropped due to RPC congestion.
DRPEMSG2 (CCS7)	Number of priority Level 2 ECIS6 messages dropped due to RPC congestion.
DRPEMSG3 (CCS7)	Number of priority Level 3 ECIS6 messages dropped due to RPC congestion.
ERSEC (CCS7)	Number of one-second intervals with at least one error.
ERSECTE (CCS7)	Threshold exceeded for ERSEC.
FORRX (CCS7)	The link expenenced a forced retransmit cycle.
FORRXBY (CCS7)	Bytes retransmitted during forced retransmit mode.
GTTPERFD (Office)	Total number of CCS7 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 no translation.
GTTUNONS	Global title translations unable to perform diagnostic 0.

Table 6-H. Valid CNI Measurement IDS (Contd)

Measurement	Description
HTXNEGAK (CCS7)	Link unavailable.
L6MGRV_ (CCS7)*	ECIS6 messages received on virtual link.
L6MGXV_ (CCS7)*	ECIS6 messages transmitted on virtual link.
L6SUPRV_ (CCS7)*	Telephone message signal units received on virtual link.
L6SUPXV_ (CCS7)*	Telephone message signal units transmitted on virtual link.
L7ACO (CCS7)	Automatic changeover.
L7ACOTE (CCS7)	Automatic changeover threshold exceeded.
L7ACOFE (CCS7)	Automatic changeover initiated by the far-end.
L7ACONE (CCS7)	Automatic changeovers initiated at the near-end.
L7AFLT (CCS7)	Duration of automatic link out-of-service including duration of declared failure.
L7BADRTG (CCS7)	Message signal units discarded due to bad or no routing data.
L7BOFR (CCS7)	The receive buffer in an SS7 link node overflows.
L7BOFRT (CCS7)	Duration of the receive buffer overflow.
L7BOLR (CCS7)	The receive buffer in an SS7 link node overloaded.
L7BOLRT (CCS7)	Duration of the receive buffer overload.
L7BYTO3B (CCS7)	SS7 message bytes sent to 3B20D computer.
L7DIF (CCS7)	CNI SS7 data integrity flag.
L7EMER (CCS7)*	Emergency restart due to local failure.
L7EMRPO (CCS7)*	Emergency restart due to far-end processor outage.
L7EMRPOT (CCS7)*	Duration of emergency restart due to far-end processor outage.
L7EMPT (CCS7)*	Duration of emergency restart due to local failure.
L7FLALIGN (CCS7)	Alignment failure.
L7FLD (CCS7)	Declared link failure.
L7FLDT (CCS7)	Duration of declared link failure.
L7LCDIS1X (CCS7)	Level 1 transmit buffer congestion discard.
L7LCDIS1XT (CCS7)	Duration of Level 1 congestion discard.
L7LCDIS2X (CCS7)	Level 2 transmit buffer congestion discard.
L7LCDIS2XT (CCS7)	Duration of Level 2 discard.
L7LCDIS3X (CCS7)	Level 3 transmit buffer congestion discard.
L7LCDIS3XT (CCS7)	Duration of Level 3 congestion discard.
L7LCON1X (CCS7)	Level 1 transmit buffer congestion onset.
L7CON1XT (CCS7)	Duration of Level 1 congestion onset.
L7LCON2X (CCS7)	Level 2 transmit buffer congestion onset.
L7LCON2XT (CCS7)	Duration of Level 2 congestion onset.
L7LCON3X (CCS7)	Level 3 transmit buffer congestion onset.
L7CON3XT (CCS7)	Duration of level congestion onset.
L7MCOFE (CCS7)	Far-end manual changeover request is received, usually due to a need for link changes or maintenance.
L7MCONE (CCS7)	Near-end manual changeover due to local maintenance action.
L7MFLT (CCS7)	Duration of manual link out-of-service.
L7MGSR (CCS7)	Non-ECIS6 messages received.
L7MGSX (CCS7)	Non-ECIS6 messages transmitted.
L7MRPBC (CCS7)*	ECIS6 message rejected due to congestion.
L7MRPNT (CCS7)*	ECIS6 message rejected due to translation data.
L7POR (CCS7)	Far-end processor outage occurred.
L7PORT (CCS7)	Duration of processor outage.
L7POX (CCS7)	Link interface in processor outage send mode.
L7POXT (CCS7)	Duration of processor outage in effect.

* CCIS6 related measurements should always be zero (0).

Table 6-H. Valid CNI Measurement IDS (Contd)

Measurement	Description
L7RBFOC (CCS7)	Average receive buffer length in bytes.
L7RTGAUD (CCS7)	Routing audit failure.
L7XBFLOOK (CCS7)	Number of transmit buffer visits by the link interface.
L7XBFOC (CCS7)	Average transmit buffer length in bytes.
MGANSRV_ (CCS7)*	Answer messages received on virtual link.
MGANSXV_ (CCS7)*	Answer messages transmitted on virtual link.
MGIAMRV_ (CCS7)*	Initial address messages received on virtual link.
MGIAMXV_ (CCS7)*	Initial address messages transmitted on virtual link.
MGMSUR (CCS7)	Message signal units received.
MGMSUX (CCS7)	Message signal units transmitted.
MRBADRTG (Office)	Message signal units discarded due to routing data error (no routing data).
MRSBCO7 (Office)*	Destination Common Channel Interoffice Signaling 6 (DCIS6) message rejected due to congestion.
MRSNTO7 (Office)*	DCIS6 message rejected due to no translation data.
MSG7LOOP (CCS7)	SS7 messages "looped" in the network.
MSINSIO (CCS7)*	Message signal units discarded due to invalid Service Indicator Byte.
MSUDISC_ (CCS7)	Messages removed due to link congestion.
MSURMV (CCS7)	Messages removed due to link congestion.
NACR (CCS7)	Negative acknowledgment "event" occurred.
NOCMG (Office)	Number of times system in state in which it could not process CCS7 messages.
NOCMGT (Office)	The accumulated time in seconds during which no messages could be processed.
NDCFLABN (CCS7)	Number of SLK declared failures due to abnormal conditions.
NDCFLHWP (CCS7)	Number of SLK declared failures due to general hardware problems.
NDCFLSWP (CCS7)	Number of SLK declared failures due to general software problems.
NDCFLXDA (CCS7)	Number of SLK declared failures due to excessive delay of acknowledgment.
NDCFLXDC (CCS7)	Number of SLK declared failures due to excessive congestion duration.
NDCFLXER (CCS7)	Number of SLK declared failures due to excessive error rate.
ORIGMSUS (CCS7)*	Originated message signal unit.
ORMSUOCT (CCS7)*	Originated message signal unit bytes.
RABT (CCS7)	Number of abort events received on the link.
RABTER (CCS7)	Number of bytes received in error during abort events.
RTESETUN (Cluster)	Route set unavailable.
RTESETUNT (Cluster)	Duration of route set unavailable.
RTGAUDFL (Office)	Routing audit failure.
SC7R (CCS7)	Signaling connection control part message received.
SC7RERPRO (CCS7)	An SCCP message destined for a prohibited subsystem.
SC7RERUA (CCS7)	An SCCP message destined for an unknown address or global title.
SC7RERUATY (CCS7)	An SCCP message destined for an unknown address or global title type.
SC7RERUNE (CCS7)	An SCCP message destined for an unequipped subsystem.
SC7GTR (CCS7)	An SCCP message destined for global title routing.
SC7LNN (CCS7)	An SCCP message destined for the local network node.
SC7RLSS (CCS7)	An SCCP message destined for an equipped local subsystem.
SC7NATL (CCS7)	Messages discarded due to blocked point code.
SC7UDSX (CCS7)	Unit data service message transmitted in response to a unit data message type failure.
SCR (Office)	An SCCP message received.
SCRERPRO (Office)	An SCCP message destined for a prohibited subsystem.
SCRERUA (Office)	An SCCP message destined for an unknown address returned.

* CCSI6 related measurements should always be zero (0).

Table 6-H. Valid CNI Measurement IDS (Contd)

Measurement	Description
SCRERUATY (Office)	An SCCP message destined for an unknown address type.
SCRERUNE (Office)	An SCCP message destined for an unequipped subsystem.
SCRGTR (Office)	An SCCP message destined for global title routing.
SCRLNN (Office)	An SCCP message destined for the local network node.
SCRLSS (Office)	An SCCP message destined for an equipped local subsystem.
SCSRTR (Office)	Subsystem routing test message received.
SCSRTX (Office)	Subsystem routing test message transmitted.
SCSSTR (Office)	Subsystem status test message received.
SCSSTX (Office)	Subsystem status test message transmitted.
SCUDSX (Office)	Unit data service message sent by message handling in central processor.
SEVERSEC (CCS7)	Severe error seconds.
SPI (CCS7)	Adjacent signaling point isolated due to local failure.
SPIA (Office)	Adjacent signaling point isolation due to local failure of A-link.
SPIAT (Office)	Duration of SPIA.
SPIPO (CCS7)	Adjacent signaling point isolation due to far-end processor outage.
SPIPOT (CCS7)	Duration of the SPIPO measurement.
SPISP (Office)	Adjacent signaling point isolated due to local failure.
SPISPT (Office)	Duration of SPI measurement.
SPIT (CCS7)	This time period begins when a linkset along a path to the indicated destination fails, causing it to be isolated.
SQL (CCS7)	Link quality.
THRSWMSU (CCS7)*	Through-switched message signal units.
TLNKACTV (CCS7)	*Signaling link active time.*
TRMDMSUS (CCS7)*	Terminated message signal units.
TRMSUOCT (CCS7)*	Terminated message signal unit bytes.
TSMSUOCT (CCS7)*	Through-switched message signal unit bytes.
UNVL (CCS7)	Link unavailable.

* Measurement is also provided as a per-office total for all SS7 links.

Table 6-I. Valid IMS Measurement IDS

Measurement	Description
ABOFL (Office)	Long message type application buffer overflow.
ABOFS (Office)	Short message type application buffer overflow.
ARRATT (NP)	Automatic ring recovery restoral attempts.
ARREXR (NP)	Automatic ring recovery restoral failure due to excessive restore rate.
ARRFLR (NP)	Automatic ring recovery restoral failures.
BLK0 (Office)	Ring 0 blockage.
BLK1 (Office)	Ring 1 blockage.
BLKG0 (NP)	Ring 0 blockage.
BLKG1 (NP)	Ring 1 blockage.
BUFSW (NP)	Ring receive buffer switch.
CONFG (NP)	Begin/end point of isolation segment.
CONFGT (NP)	Duration of begin/end point of isolation segment.
CUTOCUMSG (Office)	3B20D computer to 3B20D computer IMS messages.
CUTOCUWDS (Office)	3B20D computer to 3B20D computer IMS message words.
CUTORMSG (RPC)	3B20D computer to RPC IMS messages.
CUTORWDS (RPC)	3B20D computer to RPC IMS message words.
DMAFLT (RPC/DLN)	Direct memory access fault.
DMAMISS (RPC)	Direct memory access missed.
IDLE (NP)	A relative measure of node processor idle time.
IFBPTER0 (NP)	Interframe buffer parity error on ring 0.
IFBPTER1 (NP)	Interframe buffer parity error on ring 1.
ILLEGAL (NP)	Number of messages processed by the illegal message handler.
IMNPDIF (NP)	Node processor data integrity flag.
IMOFFDIF (Office)	Per office data integrity flag.
INBOF (NP)	Failure to obtain a new ring receive buffer.
INIT0 (Office)	Number of level 0 IMS initializations that started.
INIT0T (Office)	Duration of level 0 IMS initialization.
INIT1A (Office)	Number of level 1A IMS initializations that started.
INIT1AT (Office)	Duration of level 1A IMS initialization.
INIT1B (Office)	Number of level 1B IMS initializations that started.
INIT1BT (Office)	Duration of level 1B IMS initialization.
INIT2 (Office)	Number of level 2 IMS initializations started.
INIT2T (Office)	Duration of level 2 IMS initialization.
INIT3 (Office)	Number of level 3 IMS initializations that started.
INIT3T (Office)	Duration of level 3 IMS initialization.
INIT4 (Office)	Number of level 4 IMS initializations that started.
INIT4T (Office)	Duration of level 4 IMS initializations.
INITBT (Office)	Number of IMS boot prologues that start.
INITBTT (Office)	Duration of IMS boot prologue.
IPFMTER0 (NP)	Ring input format error on ring 0.
IPMNTER1 (NP)	Ring input format error on ring 1.
IPSM0 (NP)	Ring 0 input source match.
IPSM1 (NP)	Ring 1 input source match.
IUNOVLD0 (IUN)	Number of times the IMS user node entered overload level 0 (the normal state).
IUNOVLD1 (IUN)	Number of times the IMS user node entered overload level 1.
IUNOVLD2 (IUN)	Number of times the IMS user node entered overload level 2.
MINTRA (RPC)	Number of intra-node messages delivered.
MRINTCH (NP)	Message returned to the ring due to destination channel being closed.
MRNIAU (Office)	Automatic multiple ring node isolation.

Table 6-I. Valid IMS Measurement IDS (Contd)

Measurement	Description
MRNIAUT (Office)	Duration of automatic multiple ring node isolation.
MRNRING (NP)	Message returned from ring.
MRRGQ0 (NP)	Message received from ring 0 queued.
MRGQ1 (NP)	Message received from ring 1 queued.
MRRING (Office)	Message returned to ring with "returned message" control code (destination did not accept message).
MXRG0 (NP)	Message transmitted to ring 0.
MRRG1 (NP)	Message transmitted to ring 1.
NPPTER (NP)	Node processor parity error.
OOSAU (NP)	Automatic out of service.
OOSAUT (NP)	Duration of automatic out of service.
OOSCFG (NP)	Out-of-service due to ring reconfiguration.
OSCFGT (NP)	Duration out-of-service due to ring reconfiguration.
OOSMN (NP)	Manual out-of-service.
OOSMT (NP)	Duration of manual out-of-service.
PANICS (NP)	Number of recoverable errors.
PIOFLT (RPC/DLN)	Fault recovered after a program input/output request is issued to a ring peripheral controller.
PTERTE (NP)	Number of times soft parity error exceeded a threshold.
RACER0 (NP)	Ring access controller problem on ring 0.
RACER1 (NP)	Ring access controller problem on ring 1.
RBOF (CHN)	Single message read list buffer overflow.
RBOFBLK (CHN)	Block message read list buffer overflow.
RCOPTER0 (NP)	Ring access controller output parity error on ring 0.
RCOPTER1 (NP)	Ring access controller output parity error on ring 1.
RDFMTER0 (NP)	Ring read format error on ring 0.
RDFMTER1 (NP)	Ring read format error on ring 1.
RDINHER0 (NP)	Read inhibit error on ring 0.
RDINHER1 (NP)	Read inhibit error on ring 1.
RDWN (Office)	Entire ring down.
RDWNT (Office)	Duration of that entire ring is down.
RGCNFG (Office)	Ring containing an isolated segment.
RGNCNFGT (Office)	Duration of ring contains an isolated segment.
RINTCH (CHN)	Message returned to the ring due to closed destination channel in the central processor.
RIPTER0 (NP)	Ring interface parity error or orphan byte condition on ring 0.
RIPTER1 (NP)	Ring interface parity error or orphan byte condition on ring 1.
RNIMN (Office)	Zero or more ring nodes isolated manually.
RNIMNT (Office)	Duration of zero or more ring nodes isolated manually.
RPCBOF (RPC)	RPC buffer overflow.
RRBOVFLW0 (NP)	Number of times the ring node has reached the overflow state 0 (the normal, no discard state).
RRBOVFLW1 (NP)	Number of times the ring node has transitioned to the overflow state 1.
RRBOVFLW1T (NP)	Duration of ring receive buffer overflow state 1.
RBOVFLW2 (NP)	Number of times a ring node reached the overflow state 2.
RRBOVFLW2T (NP)	Duration of ring receiver buffer overflow state 2.
RRBOVFLW3 (NP)	Number of times the ring node has reached the overflow state 3.
RRBOVFLW3T (NP)	Duration of ring receive buffer overflow state 3.
RSTRMT (NP)	Successful restart without reload.

Table 6-I. Valid IMS Measurement IDS (Contd)

Measurement	Description
RTMSGSRC (CCS7)	Message received with a source address match.
RTOCUMSG (RPC)	RPC to 3B20D computer IMS messages.
RTOCUWDS (RPC)	RPC to 3B20D computer IMS message words.
SFPTER0 (NP)	Soft parity error on ring 0.
SFPTER1 (NP)	Soft parity error on ring 1.
SPNIAU (Office)	Automatic single ring node isolation.
SRNIAUT (Office)	Duration of automatic single ring node isolation.
WBOFN (CHN)	New write list buffer overflow.
WBOFNL (CHN)	Long new write list buffer overflow.
WBOFO (CHN)	Old write list buffer overflow.
WRRGQ0 (NP)	3B20D computer words received from ring 0 queued.
WRRGQ1 (NP)	3B20D computer words received from ring 1 queued.
WSMER0 (NP)	Write source match error on ring 0.
WSMER1 (NP)	Write source match error on ring 1.
WTFMTER0 (NP)	Ring write format error on ring 0.
WTFMTER1 (NP)	Ring write format error on ring 1.
WXRG0 (NP)	3B20D computer words transmitted to ring 0.
WXRG1 (NP)	3B20D computer words transmitted to ring 1.

7. Measurement Output Control Table

7.01 The Measurement Output Control Table (MOCT) is used to control frequency, format, content of critical messages, and measurement reports. The design of the operational, administrative, and maintenance plan for the MOCT remains the responsibility of the user, based on the specific needs of the user's network.

7.02 The MOCT consists of five separate tables:

- Critical Event Table (CET)
- Exception Table (EXCP)
- History File Descriptor Table (HFDT)
- Scheduler Table (SCHD)
- User View Description Table (UVDT).

7.03 The tables are used to manage and control various reports and measurements provided by IMS/CNI application software.

7.04 The CET table provides critical event messages on a real time basis. The remaining tables function together to generate performance measurement reports. These tables have been designed to allow user flexibility in selecting various data and thresholds to be used in generating messages and reports.

7.05 For additional information on MOCT, refer to the following documents:

- 231-390-500, *Common Channel Signal System 7, General Description, Feature Document, 1A ESS*
- 234-100-120, *Common Channel Signaling System, Common Network Interface 4ESS Switch*
- 235-190-120, *5ESS Switch Common Channel Signaling Features*
- 270-750-406, *A-I-Net STP Data Base Administration (Release 2).*

8. Displaying Routing Data (OP:C7NET)

Purpose

8.01 The **OP:C7NET** input message is a valuable tool that allows dynamic routing information to be examined on request.

8.02 This tool provides a printout of various routing data elements, depending on the options specified in the input request. Options currently available are:

(a) A report of the preferred and active routing information for all assigned clusters values (**PRTE** keyword).

(b) A report of the contents of the global title translation table (**GTXTAB** keyword).

(c) A report of the preferred and active routing information for a specific cluster (**PCLU** keyword).

(d) A report of the linkset information about the Ring Node Addresses (RNAs) that are actively being used for routing per linkset, all equipped linksets and the current linkset relations (**PLS** keyword).

(e) A report of the point codes of the two adjacent STPs and the local subsystems that are marked as receiving backup traffic from each of these adjacent STPs (**RIND** keyword).

(f) A report of all point codes contained in the SCCP broadcast list (**BRDCST** keyword).

(g) A report of all point codes contained in the SCCP permanent relations list (**RELATE** keyword).

(h) A report of the data concerning a given local subsystem (**SSINFO** keyword). Valid for 1A ESS and 5ESS switches and *A-I-Net* products STP only.

(i) A report of the local point code (**LOCPC** keyword).

8.03 Execution of this tool is invoked by the **OP:C7NET** input message. Refer to the appropriate IM/OM manuals ("Introduction") for the proper format of the **OP:C7NET** input and output messages.

8.04 The sample outputs shown in Figures 6-2 and 6-3 were generated by an **OP:C7NET** input message (**PRTE** keyword). The output data represents network configurations shown in Chapter 3, Figures 3-1 and 3-6.

```
OP:C7NET COMPL CDNETWORK = 238; CNLOCPC = 0xee2b06; CDSTDPC = 1;
+---------+---------+--------+--------+----------+
| NID     |         |        |        |          |
+---+-----|  FLAG   | PREFER | ACTIVE | DIR      |
| HEX| DEC|         | LKSET  | LKSET  | INDEX    |
+---------+---------+--------+--------+----------+
|0xee| 238| CLUSTER |        |        |     0    |
|0xfe| 254| NCLUSTER|        |        |     1    |
+-----------------------------------------------+
```

< This table is shown for 1AP3E, 5E7, and 4AP10 software releases and A-I-Net® STP RLS1.

```
+---------+----+---+-------+--------+----+-----+-----------+-+------+
| HEX     |  N | C |       | STATE  |    |     |  STATUS   |C|      |
| POINT   |  I | L |ROUTING|--------|PREF| ACT |---+---+---|O|INDEX |
| CODE    |  D | U | FLAG  |RRXCMUCS| LS | LS  |PRE|ALT|CLT|N|      |
+---------+----+---+-------+--------+----+-----+-----------+-+------+
| 0xee5000| 238| 80|     LS|00 00100|   5|    5|TFA|TFA|TFA|O|      |
| 0xee5100| 238| 81|     LS|00 00100|   6|    6|TFA|TFA|TFA|O|      |
| 0xee2b00| 238| 43|RPOPC_M|00 01000|   7|    7|TFA|TFA|TFA|O|  1   |
+---------+----+---+-------+--------+----+-----+-----------+-+------+

   +---------+---+---+---+-----+--------+----+----+-----------+-+------+
   | HEX     | N | C | M |     | STATE  |    |    |  STATUS   |C|      |
   | POINT   | I | L | E |ROUTE|--------|PREF| ACT|-----------|O|INDEX |
   | CODE    | D | U | M |FLAG |RRXCXXCS| LS | LS |PRE|ALT|CLT|N|      |
   +---------+---+---+---+-----+--------+----+----+---+---+---+-+------+
   |0xee2b07|238|43 | 7 | CLS |10 0 00 |  7 |  5 |TFR|TFA|TFA|0|      |
   +-------------------------------------------------------------------+

+---------+----+---+-------+--------+----+----+---+---+---+-+------+
| 0xee5200| 238| 82|RPOPC_C|00 00000|   7|   7|TFA|TFA|TFA|O|      |
| 0xee5300| 238| 83|RPOPC_C|00 00000|   7|   7|TFA|TFA|TFA|O|      |
| 0xee5400| 238| 84|RPOPC_C|00 00000|   7|   7|TFA|TFA|TFA|O|      |
| 0xee5500| 238| 85|RPOPC_C|00 00000|   7|   7|TFA|TFA|TFA|O|      |
| 0xee9b00| 238|155|RPOPC_C|00 00000|   7|   7|TFA|TFA|TFA|O|      |
| 0xeeeb00| 238|235|RPOPC_C|00 00000|   7|   7|TFA|TFA|TFA|O|      |
+-------------------------------------------------------------------+

+---------+----+---+-------+--------+----+-----+-----------+-+------+
| HEX     |  N | C |       | STATE  |    |     |  STATUS   |C|      |
| POINT   |  I | L |ROUTING|--------|PREF| ACT |-----------|O|INDEX |
| CODE    |  D | U | FLAG  |RRXCMUCS| LS | LS  |PRE|ALT|CLT|N|      |
+---------+----+---+-------+--------+----+-----+-----------+-+------+
| 0xfe5200| 254| 82|CPOPC_C|00 00100|   7|   7|TFA|TFA|TFA|O|      |
| 0xfe5300| 254| 83|CPOPC_C|00 00100|   7|   7|TFA|TFA|TFA|O|      |
| 0xfeeb00| 254|235|RPOPC_C|00 00000|   6|   6|TFA|TFA|TFA|O|      |
+---------+----+---+-------+--------+----+-----+-----------+-+------+
```

Figure 6-2. OP:C7NET Output Example (Sheet 1 of 2)

```
OP:C7NET COMPL CDNETWORK = 238; LOCAL PC= 0xee2b07; PC FORMAT = ANSI STANDARD;
 +---------+--------+-----+-------------------+---+-----+---+--------+
 |   NID   |        |     | ROUTES AND STATUS | C |     | R |        |
 +----+----|ROUTING |ACT  +-----+------+------+ N | RPI | C | INDEX  |
 | HEX| DEC| FLAG   |LS   |PRIM | ALT1 | ALT2 | G |     | T |        |
 +----+----+--------+-----+-----+------+------+---+-----+---+--------+
 |0xee| 238| NTWK   |     |     |      |      |   |  -  |   |   0    |
 |0xfe| 254| NTWK   |     |     |      |      |   |  -  |   |   1    |
 +-------------------------------------------------------------------+

 +---------------------+---------+-----+------------------+-+---+-+------+
 |      POINT CODE     |         |     | ROUTES AND STATUS|C|   |R|      |
 +-------------------- + ROUTING + ACT +------+------+----+N|RPI|C|      |
 | HEX     |DECIMAL    |  FLAG   | LS  | PRIM | ALT1 |ALT2|G|   |T|INDEX|
 +---------+-----------+---------+-----+------+------+----+-+---+-+------+
 | ee5000  |238-080-000 | UPOPLCU |  5  | 5A   |  6A  | 1A |0| - | |      |
 | ee5100  |238-081-000 | UPOPLCU |  6  | 6A   |  5A  | 1A |0| - | |      |
 | ee2b00  |238-043-000 | POPLCU  |  7  | 7AA  | 8AA  |    |0| - | |    1 |
<<| ee2b08  |238-043-008 | DMEMBER | BLK | 7PP  | 8AA  |    | | | | |      |
 | ee5200  | 238-082-000| POPLCU  |  7  | 7AA  | 8AA  |    |0|   | | |      |
 | ee5300  | 238-083-000| POPLCU  |  7  | 7AA  | 8AA  |    |0|   | | |      |
 | ee5400  | 238-084-000| POPLCU  |  7  | 7AA  | 8AA  |    |0|   | | |      |
 | ee5500  | 238-085-000| POPLCU  |  7  | 7AA  | 8AA  |    |0|   | | |      |
 | ee9b00  | 238-155-000| POPLCU  |  7  | 7AA  | 8AA  |    |0|   | | |      |
 | eeeb00  | 238-235-000| POPLCU  |  7  | 7AA  | 8AA  |    |0|   | | |      |
 +-------------------------------------------------------------------------+

 +---------------------+---------+-----+--------------------+-+---+-+------+
 | POINT CODE          |         |     | ROUTES AND STATUS  |C|   |R|      |
 +-------------------- + ROUTING + ACT +--------------------+N|RPI|C|      |
 | HEX     | DECIMAL   |  FLAG   | LS  | PRIM | ALT1 | ALT2 |G|   |T|INDEX|
 +---------+-----------+---------+-----+------+------+------+-+---+-+------+
 | fe5200 |254-082-000 | CLU_0   |  7  | 7AA  | 8AA  |      |0| - | |      |
 | fe5300 |254-083-000 | CLU_0   |  7  | 7AA  | 8AA  |      |0| - | |      |
 | feeb00 |254-235-000 | POPLCU  |  6  | 6AA  | 8AA  |      |0| - | |      |
 +-------------------------------------------------------------------------+
```

<This table is shown for 1AP3F, 4AP12, and 5E9 software releases and later.

Figure 6-2. OP:C7NET Output Example (Sheet 2 of 2)

```
OP:C7NET COMPL CDNETWORK = 238; CNLOCPC = 0xee5000; CDSTDPC = 1;
+---------+---------+--------+--------+---------+
| NID     |         |        |        |         |
+----+----|  FLAG   | PREFER | ACTIVE |  DIR    |
| HEX| DEC|         | LKSET  | LKSET  | INDEX   |
+----+----+---------+--------+--------+---------+
|0xee| 238| CLUSTER |        |        |    0    |
|0xfe| 254| NCLUSTER|        |        |    1    |
+-------------------------------------------------+
```

< This table is shown for A-I-Net® STP RLS 2 software.

```
+-------+----+---+--------+--------+---+-----------+-------+---+-----+
| HEX   | N  | C |        | STATE  |   | ROUTE 1   | CLK   | C | IND |
| POINT | I  | L |  ROUTE |--------|ACT|-----------|-------| O |     |
| CODE  | D  | U |  FLAG  |RRXCMUCS|LS |LS | P | A |LS |   | N |     |
+-------+----+---+--------+--------+---+---+---+---+---+---+---+-----+
|ee5100 |238 |81 |   LS   |00 00100| 0 | 0   A   A | 1   A | 0 |     |
|ee5200 |238 |82 |   LS   |00 00100| 1 | 1   A   A | 1   A | 0 |     |
|ee5300 |238 |83 |   LS   |00 00100| 2 | 2   A   A | 1   A | 0 |     |
|ee5400 |238 |84 |   LS   |00 00100| 3 | 3   A   A | 1   A | 0 |     |
|ee5500 |238 |85 |   LS   |00 00100| 4 | 4   A   A | 1   A | 0 |     |
|ee2b00 |238 |43 |RPOPC_C |00 01000| 5 | 5   A   A | 1   A | 0 |  1  |
+-------+----+---+--------+--------+---+---+---+---+---+---+---+-----+

+-------+----+---+---+-----+--------+----+---------+----+-------+-+---+
| HEX   | N  | C | M |ROUTE| STATE  |    |ROUTE 1  |CLK |ROUTE 3|C|IND|
| POINT | I  | L | E |FLAG |--------| ACT|---------|----|-------|O|   |
| CODE  | D  | U | M |     |RRXCXXCS| LS |LS |P|A |LS| |LS|P|A |N|   |
+-------+----+---+---+-----+--------+----+---+-+--+--+--+--+-+--+-+---+
|ee2b07 |238 |43 | 7 | LS_B|000 00  |  4 | 5  A A |1  P|4  A A |0|   |
+-------+----+---+---+-----+--------+----+---+-+--+--+--+--+-+--+-+---+

+-------+----+---+--------+---------+----+---------+-----+---+-----+
| HEX   | N  | C |        | STATE   |    | ROUTE 1 | CLK | C | IND |
| POINT | I  | L |  ROUTE |---------| ACT|---------|-----| O |     |
| CODE  | D  | U |  FLAG  |RRXCMUCS | LS |LS|P| A |LS|  | N |     |
+-------+----+---+--------+---------+----+--+-+---+--+--+---+-----+
|eeeb00 |238 |235| RPOPC_C| 00 01000|  3 |3 | A   A |1  A | 0 |     |
+-------+----+---+--------+---------+----+--+-+---+--+--+---+-----+

+-------+----+---+--------+--------+-----+---------+-----+-+-----+
| HEX   | N  | C |        | STATE  |     | ROUTE 1 | CLK |C| IND |
| POINT | I  | L |  ROUTE |--------| ACT |---------|-----|O|     |
| CODE  | D  | U |  FLAG  |RRXCMUCS| LS  | LS|P|A| |LS|  |N|     |
+-------+----+---+--------+--------+-----+---+-+-+-+--+--+--+-+-----+
|fe5200 |254 |82 |   LS   | 0000100| 6   | 6  A A  |1  A |0|     |
|f35300 |254 |83 |   LS   | 0000100| 7   | 7  A A  |1  A |0|     |
|feeb00 |254 |235|RPOPC_C | 0001000| 8   | 8  A A  |1  A |0|     |
+-------+----+---+--------+--------+-----+---+-+-+-+--+--+--+-+-----+
```

Figure 6-3. OP:C7NET Output Example (*A-I-Net* STP, RLS 2)

8.05 In the previous example (Figure 6-2), the switch signals over linkset 5 to the adjacent STP with a point code 225080000 and over linkset 6 to the adjacent STP with a point code 225081000. Traffic over these linksets is allowed since the preferred and active routes are identical and the routing status indicates Transfer Allowed (TFA).

8.06 Traffic to clusters 155 and 235 within the network 238 is load-shared over combined linkset 7. Traffic over combined linkset 7 is allowed since the preferred and active routes are identical and the routing status indicates TFA.

NOTE 1:

The routing flag to clusters 155 and 235 indicates RPOPC_C. This dictates that dynamic member-level routing will be maintained for clusters 155 and 235. In the event that signaling to a single member within one of these clusters is prohibited, signaling to other members (if any) of the same cluster will not be affected.

NOTE 2:

If the routing flag indicates Combined Linkset (CLS), dynamic cluster-level routing will be maintained for the cluster. In the event that signaling to a single member within the cluster is prohibited, signaling to other members (if any) of the same cluster is also prohibited. The CLS routing for clusters is typically used for routing to nonadjacent STPs.

CAUTION:

Because this tool is also used to print routing information for the Lucent Technologies network, it is important that the American National Standards Institute (ANSI) point code indicator "STD_PC" be set to 1 in the CNI Network File. You can see what the ANSI point code indicator is set by observing the value of CDSTDPC in the line of any *OP:C7NET* output.

9. Message Transfer Part Routing Verification Test

Purpose

9.01 The Message Transfer Part (MTP) Routing Verification Test (MRVT) is intended to specifically address the problems of administering and maintaining the SS7 network. The MRVT is a means of verifying MTP routing data between signaling points (SPs) in an SS7 network. It confirms all MTP routes between an "initiating SP" (the initiator) and a "terminating SP" (the terminator) and reports the findings back to the initiator. The initiator and terminator can be any of the following, all of which must support MRVT capabilities:

- Switches
- Service Control Points (SCPs)
- Signaling Transfer Points (STPs).

9.02 The SPs along a route between the initiator and terminator SPs are known as intermediate SPs and are always STPs.

NOTE:
All signaling points along the path from the initiator to the terminator (inclusive) must support MRVT for the test to work correctly.

9.03 The actual routes used by the MRVT are determined by the MTP routing data defined within the SPs of the network. The routing data in a given SP specifies one or more possible candidates for the next SP to which a message bound for a specific designation is forwarded.

9.04 The MRVT checks the accuracy and consistency of the *administrable* MTP routing data at all the SPs involved in routing between a given source and destination. Administrable routing data is "static" routing data that can be modified directly through a recent change mechanism.

9.05 The MRVT does not check *dynamic* routing data, which is routing data in effect at any given time. Dynamic routing data is determined not only by the static routing data, but also by the history of processor, link failures, and recoveries in the network.

NOTE:
When shown alone, the acronym MRVT refers to the test itself. The phrase "MRVT message" refers to the MRVT test message. The term "MRVT user" refers to a person or Operations System (OS) that runs an MRVT.

9.06 Table 6-J lists the available generic software releases for Lucent Technologies products.

Table 6-J. MRVT Generic Software Releases

1A ESS™ Switch 1APS	4ESS™ Switch APS	5ESS® Switch	*A-I-Net*® STP
1AP3C or later	4AP8 or later	5E6 or later	Release 0 or later

Overview of the MTP Routing Verification Test

9.07 A fundamental part of the MRVT is the ability to access administrable MTP routing data at each SP in order to make certain determinations:

(a) At an initiating SP or intermediate SP, whether or not the terminating SP point code is known

(b) At an intermediate SP or terminating SP, whether or not the initiating SP is known

(c) At an initiating SP or an intermediate SP, determination of the point code(s) of the adjacent SP(s) which lie on route(s) to the terminating SP

(d) At an initiating SP or an intermediate SP, determination as to whether or not a particular adjacent SP of a specified point code is accessible.

9.08 For Lucent Technologies' initial MRVT implementation:

(a) MRVT procedures access *administrable* MTP routing data.

(b) A point code is deemed inaccessible if it is blocked (that is, there are no in-service signaling links to that point code) and/or resides in a different network.

(c) C-link routes are excluded from consideration in selecting routes to the terminating SP, except in the case(s) where the C links directly connect the initiating SP and the terminating SP.

9.09 The MRVT uses three SS7 Operations, Maintenance and Administration Part (OMAP) messages:

(1) MTP Routing Verification Test message

— Initiates the test of administrable MTP routing data.

(2) MTP Routing Verification Acknowledgement (MRVA) message

(1) Acknowledges each MRVT message and encodes a summary of partial test results.

(3) MTP Routing Verification Result (MRVR) message

— Conveys detailed test results to the initiator

— Reports errors found in the network and also unexpected message errors.

9.10 In an MRVT, all the signaling nodes in the test path between the initiator and terminator actively participate in the test. The SP initiating the MRVT sends an MRVT message to each adjacent SP that appears on a route to the terminator.

9.11 Figure 6-4 shows the MRVT message propagating its way in an example "quad STP" arrangement. The MRVT is initiated from switch (1) to switch (6). The STPs (2), (3), (4), and (5) are intermediate signaling points.

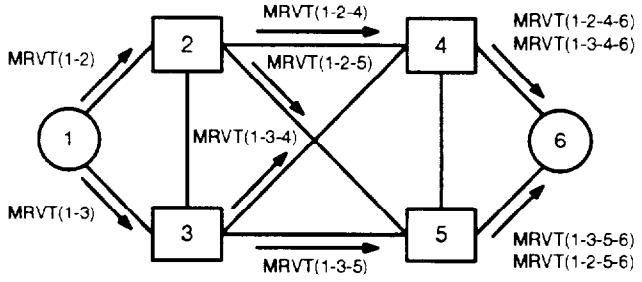


Figure 6-4. An Example of MRVT Message Flow During an MRVT

NOTE:

A sequence of numbers enclosed in parentheses shows the path of MRVT message transmissions associated with the message indicated. The first number represents the initiator, and the last number represents the MTP destination of the message. The sequence of any numbers between the first and last represents the sequence of STPs crossed.

9.12 One MRVT message arrives at the terminator for each working route. In Figure 6-5, there are four routes available from SP (1) to SP (6):

- 1-2-4-6
- 1-2-5-6
- 1-3-5-6
- 1-3-4-6.

⇒ NOTE:
Routes involving the "C" linksets 2-3 and 4-5 are not considered because "C" links are currently excluded from MRVT routes.

9.13 The propagation of MRVT messages through the network sets into motion the MRVT acknowledgment processes. The MRVA and MRVR messages involved in the acknowledgment process notify the test source of specific routes that fail, reasons for failure, and optionally, specific routes that work. Possible reasons for an MRVT failure include:

(a) Detected routing loop

(b) Excessive length route

(c) Unknown terminator SP

(d) Unknown initiator SP

(e) Recognizable but inaccessible SP

(f) Local problems in SPs (for example, processing problems)

(g) Network blockage and congestion

(h) MRVA timeout

(i) Routing data forward to the terminator is missing

(j) Routing data backward to the originator is missing.

9.14 While following all possible routes to reach the terminator from the initiator, the MRVT tracks the identities of all STPs crossed. This information, known as the *trace list*, does not include the initiator or terminator. This list will be provided when either of the following conditions are true:

(a) When the **TRACE** parameter is included in the initial request command.

(b) Test result was **PARTIAL SUCCESS**.

9.15 In Figure 6-5, the trace of MRVT (1-3-4-6) consists of STPs (3) and (4). The trace of MRVT (1)-(2) is empty.

9.16 When the test terminating SP is reached, it performs its MTP routing tests and sends an MRVA message to the SP that sent it the MRVT message. An intermediate SP sends an MRVA message to the SP that sent it the MRVT message after:

(1) The intermediate SP receives all MRVAs it is expecting, or

(2) An MRVA time-out occurs.

9.17 Figure 6-5 illustrates the MRVA messages propagating through the example network under normal operating conditions.

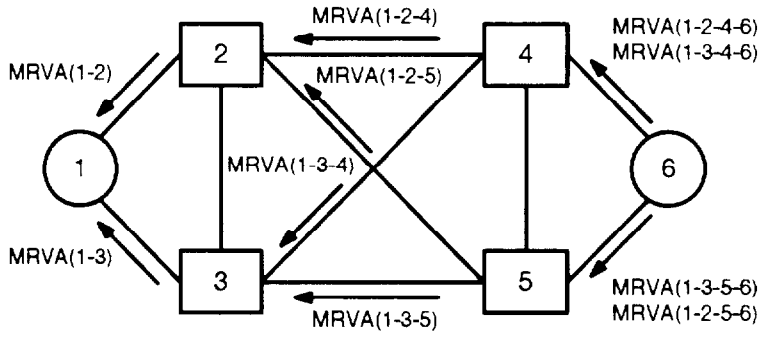


Figure 6-5. MRVA Message Flow Corresponding to Figure 6-4

9.18 The test terminating SP can optionally send an MRVR message containing the test route trace information to the test initiating SP. However, if there is a fatal error in any SP along a test route, an MRVR message is sent to the initiator and testing beyond this route is ended. When the MRVT has a result of **SUCCESS**, all possible forward and return routes that a message can take between the originating and the terminating signaling nodes are verified. For incomplete tests, all routes have been attempted.

9.19 To initiate an MRVT, the craft command **EXC:MRVT** is entered at the initiator either on-site or through a support system. The input command is broken down as shown in Table 6-K.

Table 6-K. MRVT Input Message Command for Lucent Technologies Switches

Signaling Point	Input Message
1A ESS™ Switch	**EXC:MRVT;PC a [,STPS b] [,TRACE]**
4ESS™ Switch	**EXC:MRVT;PC a [,STPS b] [,TRACE]**
5ESS® Switch	**EXC:MRVT:PC=a [,STPS=b] [,TRACE]**
A-I-Net® STP	**EXC:MRVT:PC=a [,STPS=b] [,TRACE]**

Explanation:

a = Point Code (PC) of the terminating node for the test. If an STP is the terminator, a capability code (sometimes referred to as an alias point code) may be used.

b = Value of the parameter N, which is the maximum number of STPs the MRVT is allowed to cross. The value of N should reflect the presence of the initiator if the initiator is an *A-I-Net* products STP. The default value for N is **2**.

TRACE = Keyword that determines if the path of STPs crossed by the MRVT is traced and included in the output message. If the keyword is present, the path is traced and included in the output. If the keyword is not present, traces of STPs crossed are only included in the output message when a partial success occurs.

9.20 The MRVT software in Lucent Technologies' *A-I-Net* products STP and switching products recognize any of the following local terminals and support systems as possible sources of the MRVT initiation command:

(1) Local Maintenance Terminals (MCRTs)

(2) Local non-MCRTs

(3) Local Administrative Terminals

(4) Total Network Management System (TNM)

(5) Remote Memory Administration System

(6) Signaling Engineering and Administration System for the *A-I-Net* products STP.

9.21 The results of the MRVT are reported at the initiating SP or at the OS that initiated the test. The MRVT results are not printed at intermediate or terminating SPs. An output message indicating unexpected MRVR is printed at any node that receives an unexpected MRVR. This message may also be output at an OS.

MRVT Messages

A. The MRVT Message

9.22 An MRVT message is sent from one SP to an adjacent SP. The MRVT message propagates by MTP routing over any available signaling route. The MRVT message is transmitted over a direct SS7 link to the adjacent SP unless all direct SS7 links are unavailable. If this happens, the message is sent, if possible, by a pathway with one or more intervening STPs.

9.23 The MRVT message contains the following information:

(a) Information identifying the message as an MRVT message, including a value that determines that ANSI Transaction Capabilities Application Part (TCAP) encoding is used for the message. The message is sent as a **Query With Permission** message.

(b) Point Code of the terminator.

(c) Point Code of the initiator.

(d) The TCAP Transaction Identification (ID) value. The SP transmitting an MRVT message selects the Transaction ID value for that message such that the value uniquely distinguishes that message among all outstanding (unacknowledged), transmitted OMAP **Begin/Query With Permission messages**, including other MRVT messages transmitted by the sending SP.

(e) Parameter **N**, which specifies the maximum allowed number of STPs crossed. N includes the initiator if it has an STP function.

(f) Trace Request Flag, which indicates whether Trace List information must be reported to the user. When the Trace Request Flag is TRUE, for each route that may be used to reach the terminator, the terminator must return an MRVR message containing Trace List information to the initiator. When the Trace Request Flag is FALSE, the terminator does not return any MRVR messages containing Trace List information to the initiator, unless a failure occurs.

(g) Trace List, which is an ordered list of the Point Codes (PC) of the STPs, if any, thus far encountered in the propagation of MRVT messages from the initiator up to the current SP.

B. MRVT Results

9.24 While testing all possible routes to reach the terminator from the initiator, the MRVT tracks the identities of all STPs crossed. The PC of each STP crossed can be reported to the user via one of three following output message formats.

(1) Format 1 is used when the MRVT is **successful** and the MRVT user has not requested a trace.

Format 1:

EXC:MRVT PC a STPS b NO TRACE SUCCESS

(2) Format 2 is used when the MRVT is successful and the user requested a trace.

Format 2:

EXC:MRVT PC a STPS b TRACE SUCCESS
STPS CROSSED
c
c
:
:

(3) Format 3 is used when either a partial success or failure occurs. An MRVT is stopped at the terminator or any intermediate SP at which an error is detected.

Format 3:

EXC:MRVT PC a STPS b d e
STPS CROSSED
c
:
:
ERRORS DETECTED
f g
h
:
:

Explanation:

a = The PC of the terminating node for the test.

b = Value of the parameter N, which is the maximum number of STPs the MRVT is allowed to cross. The default value is **2**.

c = List of STP point codes in the trace of a received MRVR message indicating success. If multiple MRVR messages indicating success are received, this line is printed for each such message (that is, three MRVR messages indicating success result in three lists of point codes).

NOTE:
In Format 3, if **e** indicates FAILURE, item **c** is not preset in the output.

d = TRACE if the user requested a trace of all the STPs crossed.
e = PARTIAL SUCCESS, or FAILURE depending on the responses received.
f = One of the following text phrases that describe the problem found:

- LOOP
- EXCESSIVE LENGTH ROUTE
- UNKNOWN TERMINATOR POINT CODE
- INACCESSIBLE SIGNALING POINT
- TIMER EXPIRED
- UNKNOWN INITIATOR POINT
- TEST CANNOT BE RUN DUE TO LOCAL CONDITIONS.

g = Error number associated with error described in **f**.

h = The PC(s) associated with the failure being reported.

- If **f** = LOOP, **h** = PC of SP detecting the loop followed by the list of PCs in the loop.
- If **f** = EXCESSIVE LENGTH ROUTE, **h** = PC of the SP detecting the excessive length route followed by the PCs in the loop.
- If **f** = UNKNOWN TERMINATOR POINT CODE, **h** = PC of SP that does not know the terminator.
- If **f** = INACCESSIBLE SIGNALING POINT, **h** = PC of the SP that cannot access the inaccessible SP followed by the PC of the inaccessible SP.
- If **f** = TIMER EXPIRED, **h** = PC of the SP where the timer expired followed by the list of PCs from which expected MRVA messages are not received.
- If **f** = UNKNOWN INITIATOR POINT, **h** = PC of the reporting SP followed by the PC of the SP that does not know the initiator.
- If **f** = TEST CANNOT BE RUN DUE TO LOCAL CONDITIONS, **h** = PC of the SP that cannot run the test.

NOTE:
If multiple errors are detected, items **f**, **g**, and **h** are printed for each error received.

C. MTP Routing Verification Acknowledgment Message

9.25 The second means by which the initiator learns about route status is the MTP Routing Verification Acknowledgment (MRVA) messages. An SP that receives an MRVT message from a neighboring SP always transmits an MRVA message to the neighboring SP that sent the MRVT to acknowledge its receipt.

9.26 An SP always sends an MRVT to the next SP, then waits to receive an acknowledging MRVA before sending an MRVA message to the SP that sent it the MRVT. Therefore, if all routes to the terminator are functioning properly, the first MRVA message is transmitted from the terminator itself. That MRVA message retraces the path of the MRVT and spawns MRVA messages back towards the initiator.

9.27 When an SP detects an error from the contents of an MRVT message, the SP does not transmit an MRVT message to a neighboring SP. Instead, the SP immediately transmits an MRVR message to the initiator, followed by an MRVA message to the adjacent SP that sent it the MRVT. The MRVA message contains appropriate indications of the error.

9.28 An SP waits only a limited amount of time (the value of timer T1) to receive and process all outstanding MRVA messages that correspond to a received MRVT message. If any outstanding MRVA messages are not received and processed by then, an error condition probably exists. The SP transmits an MRVA message with appropriate indications to the adjacent SP that sent the MRVT message.

9.29 The information encoded within an MRVA message does not include trace information. Error indications in MRVA messages collected by an SP are appropriately transferred to the MRVA message which the SP transmits. By this means routing error information eventually reaches the initiator through converging MRVA messages. This is done within a known amount of time allowed for the MRVT to complete.

9.30 The generation of MRVA messages requires OMAP-level processing at each SP. This is a relatively slow process. Remember also that an SP always sends MRVR messages, when required, before sending an MRVA. Since MRVRs are generated much more quickly than MRVAs, the initiator should receive MRVRs before it receives MRVAs.

9.31 The MRVA contains the following information:

(a) Information identifying it as an MRVA message. The message is sent as an ANSI **Response** message.

(b) Information indicating whether an MRVR message has been sent to the initiator in the case of failure or partial success.

(c) Transaction ID value, as specified in the received MRVT message being acknowledged. When an SP receives an MRVA message, the SP uses the Transaction ID value in that message to correlate the MRVA message with the previously transmitted MRVT message being acknowledged.

(d) Information indicating the test result at the SP which sends the message:

(1) **success**: No errors are detected by the SP through the reception of Unitdata Service (UDTS) messages or otherwise, no errors are indicated in MRVA messages received at the SP, and all expected MRVA messages are received and processed by the SP before the expiration of its timer T1.

(2) **partial success**: The SP received at least one MRVA message indicating success before the expiration of timer T1, but not all conditions for success are met.

(3) **failure**: either of the following.

— The SP had expected to receive at least one MRVA message before the expiration of timer T1, but did not receive any MRVA messages indicating success or partial success before the expiration of timer T1.

— The SP is the terminating SP and does not know the point code to the initiator.

(e) In the case of failure or partial success, additional information is provided through one or more of the following indications:

(a) **DETECTED LOOP**: A loop is detected if an adjacent SP to which an MRVT message would normally be sent is listed in the trace of the corresponding received MRVT message.

(b) **EXCESSIVE LENGTH ROUTE**: The number of SPs listed in the trace of a received MRVT message (STPs crossed) equals the value of the parameter N encoded in the message.

(c) **UNKNOWN TERMINATOR POINT CODE**: The point code of the tested destination is not recognized by MTP routing tables.

(d) **INACCESSIBLE SIGNALING POINT**: An SP is determined to be inaccessible if:

— It is blocked (all routes to the SP are unavailable).

— Non-SS7.

— Across a network boundary

— The MRVT message is rejected (that is, a UDTS message is received).

(e) **TIMER EXPIRED**: Not all expected MRVA messages are received and processed within the calculated T1 timing period.

(f) **UNKNOWN INITIATOR POINT CODE**: The point code of the initiator is not recognized by MTP routing tables.

(g) **TEST CANNOT BE RUN DUE TO LOCAL CONDITIONS**:

— Unavailability of local processing resources.

— Exceeding the maximum number of tests at a node.

— An unspecified local problem (unspecified because it is implementation-specific).

D. MTP Routing Verification Result Message

9.32 An MRVT message records in order the identities of the SPs whose successive MRVR message transmissions have led to the message's existence. The embedded list of STPs crossed is called the "trace." By this means, the MRVR message is a mechanism by which the initiator learns about the status of tested routes to the terminator.

⇒ NOTE:
The trace begins with the initiating SP if it is an STP; otherwise the trace includes only intermediate SPs. Each intermediate SP augments the trace by adding its own identity, an SS7 PC to those of the preceding SPs.

9.33 The trace in a received MRVT message indicates a route back to the initiating SP. If the receiving SP is the terminator, the terminator determines that a route from the initiator works. Alternatively, the receiving SP can detect from the trace a routing error, such as a loop or an excessive number of loops.

9.34 The receiving SP can also experience an error in its own MRVT processing. The finding of either a working route or an error is an MRVR. An SP that detects an MRVR can encode the result in an MRVR message. The MRVR message contains the trace from the received MRVT message. Included in this are any failure indications and/or other items as described in the following paragraphs.

9.35 Any SP that detects an error sends an MRVR message to the initiator if possible. A terminating SP that identifies an operable route sends an MRVR message only if the initiator has specified the **TRACE** option on the command line.

9.36 An MRVR message contains the following information:

(a) Information identifying the message as an MRVR message. The message is sent as an ANSI TCAP **Query With Permission** message.

(b) The TCAP Transaction ID. The Transaction ID is selected by the SP that transmits the MRVR message. It may not be the same as the Transaction ID found in the MRVT message being acknowledged.

(c) Point Code to the terminator.

(d) Information indicating the test result: success or specific failure type.

(e) The information field, the contents of which depend on the test result as follows:

(1) If the result of the test is **SUCCESS**:

— The Trace List contained in the received MRVT message.

(2) If the result of the test is **LOOP**:

— The Point Codes of the STPs that are in the loop.

(3) If the result of the test is **EXCESSIVE LENGTH ROUTE**:

— PC of the STPs crossed, as contained in the MRVT message.

(4) If the result of the test is **UNKNOWN TERMINATOR POINT CODE**:

— No additional information.

(5) If the result of the test is **INACCESSIBLE SIGNALING POINT**:

— The Point Code of the inaccessible SP.

(6) If the result of the test is **TIMER EXPIRED**:

— The identity of the SP(s) from which an MRVA message is not received by the time expected.

(7) If the result of the test is **UNKNOWN INITIATOR POINT CODE**:

— The point code of the SP returning the MRVA message which causes the MRVR message to be sent.

(8) If the result of the test is **TEST CANNOT BE RUN DUE TO LOCAL CONDITIONS**:

— No additional information.

MRVT Procedures at the Test-Initiating Signaling Point

9.37 This section describes the MRVT procedures performed at the SP that initiates the MRVT.

9.38 The MRVT procedure is started either (1) on demand from local maintenance staff or an operations/maintenance center or (2) on reception of an MRVT message.

9.39 It is recommended that an MRVT be performed:

(a) When MTP routing data is introduced. Each signaling point should successfully pass the MRVT procedure before being opened to network signaling traffic.

(b) When MTP routing data is changed. This validates that the change was made correctly.

(c) Periodically at an SP (having an STP function) to detect cases of mutilation of routing data.

NOTE:
This period is network dependent and should be such that the load on the network is not seriously increased.

A. Initiation of the MRVT Procedure at a Signaling Point

9.40 An MRVT is initiated at an SP in response to an MRVT initiation command from a local or remote craftsperson or administrator (the MRVT user). The parameters of this command are:

(a) The identity of the terminating SP.

(b) The maximum number of SPs between the initiator and the terminator on a valid MTP route. This number equals the value of the MRVT parameter N. This is the maximum allowed number of STPs crossed.

NOTE:
If the initiator is an STP, it must be counted when determining the value of N.

(c) The type of result information expected from the terminator, that is, whether terminator should send an MRVR message to the initiator when the result is **success**.

B. Initial Actions

9.41 On receiving the MRVT initiation command, the System Management Application Process (SMAP) immediately responds to the user with an acknowledgment message that indicates whether the command is accepted or rejected. The possible reasons for rejection include:

(a) The SP is currently participating either as an initiator or intermediate SP in an MRVT for which the terminator is the same as that named in the initiation command.

(b) The SP is already the initiator of five currently running MRVTs.

NOTE:
A limit of five is imposed to prevent the excessive use of the SP's processing resources.

(c) The value of parameter "**N**" is outside the valid range.

(d) There is some local, implementation-specific problem at the SMAP level.

If the MRVT initiation command is accepted, the SP consults its data base of *administrable* MTP routing data through the "Known Point Codes Interface" and the "List Routes Interface." These interfaces inform the SP whether or not the named terminator is known, and, if so, which adjacent SPs are on recognized MTP routes to the terminator. The list of these adjacent SPs is termed "List A." If the initiator is an *A-I-Net* products STP, the mate STP is excluded from List A. List A includes the terminator itself if the terminator is adjacent.

9.42 If the named terminator is the same as the initiating SP or the named terminator is unknown, the result is **failure.**

9.43 If the named terminator is known and it is not the same as the initiator, the initiator consults its routing data through the "Point Code Accessibility Interface" to determine which of the SPs in List A are either:

- Blocked (all MTP routes to the SP are unavailable)
- Non-SS7
- Across a network boundary, which is evident from the "network identifier" field in the point code.

The SPs with any of these characteristics are regarded as inaccessible. The initiator sends an MRVT message to all other SPs in List A. The initiator expects to eventually receive from each of these SPs an MRVA message in acknowledgment. If any of the SPs are not equipped for the MRVT, the SP in question replies to the initiator with a UDTS indication and is regarded as inaccessible. The initiator allots a maximum waiting time for the reception and processing of expected MRVA messages. This maximum is

the duration of timer T1. The timer starts as soon as it sends the MRVT messages. The duration of T1 is set as prescribed later in the "The Definition and Setting of the Timer T1" section (see paragraph 9.65).

C. Subsequent Actions

9.44 The subsequent actions of the initiating SP are grouped into two sets:

(1) Processing of received MRVR and MRVA messages

(2) Delivery of the MRVT results to the user

Processing Received MRVR and MRVA Messages

9.45 The MRVA and MRVR messages received before timer T1 expires are stored by the SP. If an expected MRVA message is received after T1 expires, it is ignored. The reception of all expected MRVA messages automatically stops timer T1.

9.46 An MRVR message received after T1 expires is treated as unconnected with the MRVT (see the "Reception of an Unexpected MRVR Message" part). Because MRVRs are generated and returned to the initiator faster than MRVAs, most MRVR messages connected with the MRVT are returned to the initiator before an MRVA message is received.

NOTE:
It is understood that MRVA and MRVR messages received during two or more concurrent MRVTs are correctly associated with their respective MRVTs through the relevant protocol message fields.

Further instructions for the processing of MRVA and MRVR messages are contained in the "MRVT Procedures at the Test-Initiating Signaling Point" part.

Reporting MRVT Results to the User

9.47 The MRVT results are derived from the contents of all MRVA and MRVR messages received before the expiration of timer T1 plus conditions identified by the initiating SP itself. These conditions include unknown terminator point code, the inaccessibility of specific SPs in List A.

9.48 The results of the MRVT results are divided into three parts for presentation to the user:

(1) The summary result of the MRVT: **success**, **partial success**, or **failure**
(2) The traces of MRVR messages sent by the terminator in cases of **partial success** or per request of the user
(3) Detailed information about error conditions encountered in the network during the MRVT.

9.49 The summary result of the MRVT is **success** only if all of the following occur:

(a) All SPs in List A are accessible.

(b) All expected MRVAs are received and processed before timer T1 expires.

(c) All received MRVAs indicate **success**.

9.50 The summary result of the MRVT is a **partial success** if either:

(a) At least one expected MRVA message indicating **partial success** is received and processed before timer T1 expires.

(b) At least one expected MRVA message indicating **success** is received and processed before timer T1 expires:

(a) One or more SPs in List A are accessible.

(b) Timer T1 expires before all expected MRVA messages are received and processed.

(c) **Failure** is indicated by one or more MRVA messages received and processed before timer T1 expires.

⇒ NOTE:
The summary result of the MRVT is **failure** if the conditions for **success** or **partial success** are not met.

The format of the MRVT result output message to the user is given in the "MRVT Messages" part. A brief summary of each format follows:

(a) If the summary result is **success** and the user has not requested MRVR messages from the terminator in cases of **success**, then only the summary result is provided to the user.

(b) If the summary result is **success** and the user has requested MRVR messages from the terminator in cases of **success**, then the traces of these MRVR messages are provided to the user in addition to the summary result.

(c) If the summary result is **partial success** or **failure**, then, in addition to the summary result, the result output message provides the user with a detailed list of detected errors and the SPs which detected them (including the initiating SP, if applicable). If the user has requested MRVR messages from the terminator in cases of success, the result output message also provides the traces of these messages.

⇒ NOTE:
The MRVT result output message is delivered to the user when all MRVA messages are received or timer T1 expires, whichever one happens first.

MRVT Procedures at an Intermediate Signaling Point

9.51 An STP becomes an intermediate SP on reception of an MRVT message from an adjacent SP. If a switch or data base receives an MRVT message which names a terminator different from the switch or data base, an error has occurred. The message is ignored.

A. Initial Actions on Reception of an MRVT Message

9.52 The following actions are performed in order:

(1) The intermediate SP consults its data base of *administrable* MTP routing data. It determines whether or not the named terminator is known, and, if so, which adjacent SPs are on recognized MTP routes to the terminator. The list of these adjacent SPs is termed "List A" and includes the terminator itself if the terminator is adjacent. List A does not include the mate *A-I-Net* products STP.

(2) The intermediate SP determines whether the test can be run. Either of two conditions precludes the running of the test:

— The intermediate SP is already participating as an intermediate SP in 25 MRVTs.

NOTE:
The limit of 25 concurrent MRVTs is imposed to guard against exhaustion of the *A-I-Net* products STP's processing resources. Two or more of these 25 can have the same terminator or the same initiator. However, no two of the 25 MRVTs can have both the same initiator and the same terminator.

— There is some local, implementation-specific problem which prevents the test from being run.
If the test cannot be run and the named initiating SP is recognized, the intermediate SP sends an MRVR message to the initiating SP and sends an MRVA message to the adjacent SP from which the MRVT message was received. These MRVA messages indicate **test cannot be run due to local conditions**.

— If the test can be run, and

(a) The initiating SP's point code is not recognized:

— The intermediate SP acknowledges the received MRVT message by sending an MRVA message to the adjacent SP from which the MRVT message was received. This MRVA message indicates **unknown initiating point code** and **MRVR not sent**.

— There is no further MRVT processing in connection with the received MRVT message.

(b) The initiating SP's point code is recognized, but the terminating SP's point code is not recognized:

— The intermediate SP sends an MRVR message to the initiator. This message is formatted with the indication **unknown terminator point code**.

— The intermediate SP acknowledges the received MRVT message by sending an MRVA message to the adjacent SP from which the MRVT message was received. This MRVA message is formatted with the indication **unknown terminator point code**.

— There is no further processing in connection with the received MRVT message.

(c) The point codes of the initiating and terminating SPs are both recognized, the intermediate SP compares the trace in the received MRVT message with its own List A, as follows:

— If a point code in List A is also in the trace, then a routing loop has been detected. The intermediate SP sends an MRVR message to the initiator containing the point codes of the SPs in the loop. Only one MRVR message is sent regardless of the number of loops detected. The intermediate SP then sends a *loop* MRVA message to the adjacent SP that sent it the MRVT message. No further processing of the MRVT is performed.

— If no routing loop is detected, but the number of point codes in the trace equals N (this is the maximum allowed number of STPs crossed), then an excessive length route is detected. An MRVR message is sent to the initiator and an MRVA message is sent to the adjacent SP that sent the MRVT message. Both messages indicate **excessive length route**. No further processing of the MRVT is performed.

— If no routing loop or excessive-length route is detected, the intermediate SP consults its dynamic routing data. This is done to check if any of the SPs in List A are inaccessible. If there are any inaccessible SPs, the intermediate SP sends an MRVR message indicating **inaccessible SP** to the initiator and an MRVA message indicating **inaccessible SP** to the adjacent SP that sent it the MRVT message. The MRVR message contains the point code of the inaccessible SP. Only one MRVR message is sent even if more than one inaccessible SP is detected. No further processing of the MRVT is performed.

— In the absence of any of the above error conditions, the intermediate SP sends an MRVT message to each SP in List A. In formatting outgoing MRVT messages, the intermediate SP copies all the information from the received MRVT message. The SP then adds its own point code to the end of the copied trace. The intermediate SP expects to receive an MRVA message from each SP in List A. If any of these SPs are not equipped to handle an MRVT, that SP replies to the intermediate SP with a UDTS indication and is considered inaccessible.

The intermediate SP allots a maximum waiting time for the reception and processing of the expected MRVA messages. This maximum is the duration of timer T1. The intermediate SP starts timer T1 as soon as it sends the MRVT messages. The duration of timer T1 is **not** the same as the duration of timer T1 at the initiator. A special formula as stated in the "The Definition and Setting of the Timer T1" part determines the duration of the intermediate SPs timer T1.

B. Subsequent Actions

9.53 The following actions occur after the sending of MRVT messages to the SPs in List A:

(1) The processing of MRVA messages received from the SPs in List A

(2) The sending of MRVR messages to the initiator in response to received MRVA messages which indicate **unknown initiator point code**

(3) The sending of an MRVA message to the adjacent SP from which the MRVT message was received.

The Processing of Received MRVA Messages

9.54 The contents of each MRVA message received before the expiration of timer T1 are stored by the SP. If an expected MRVA message is received after timer T1 expires, then the message is ignored. It is understood that MRVA messages received during the concurrent processing of two or more MRVT messages are associated with their respective MRVT message through the relevant protocol fields.

9.55 The reception of all expected MRVA messages stops timer T1.

The Sending of MRVR Messages

9.56 If the intermediate SP receives an MRVA message which indicates "unknown initiator point code" and indicates that an MRVR message was not sent, then the intermediate SP sends an MRVR message to the initiator. This MRVR message is formatted to indicate "unknown initiator point code" and contains the point code of the

SP from which the MRVA message was received. A separate MRVR message is sent for every received MRVA message of this type. Should the intermediate SP receive an MRVA message which indicates "unknown initiator point code" and indicates that an MRVR message was sent, then no MRVR message is sent in response to the received MRVA message.

The Sending of the MRVA Message

9.57 When the intermediate SP has received and processed all expected MRVA messages, or when T1 expires, whichever comes first, the intermediate SP formats an MRVA message and sends it to the adjacent SP from which the MRVT message was received. All MRVR messages are sent before the MRVA message.

9.58 The MRVA message sent indicates **success** if and only if both the following conditions are met:

(1) All MRVAs expected from the SPs in "List A" are received and processed before T1 expires.

(2) All received MRVAs indicate "success."

The MRVA message sent indicates **partial success** if either:

(1) At least one expected MRVA message indicating **partial success** is received and processed before T1 expires.

(2) At least one expected MRVA message indicating **success** is received and processed before T1 expires and either:

— One or more SPs in "List A" are inaccessible.

— Timer T1 expires before all expected MRVA messages are received and processed.

— **Failure** is indicated by one or more MRVA messages received and processed before T1 expires.

9.59 The MRVA message indicates **failure** if neither the conditions for **success** nor for **partial success** are met. The MRVA message indicates every type of error condition indicated by the MRVA messages received and processed before T1 expired. If expired. The contents of the MRVA message can be regarded as the "logical OR" of all error conditions encountered. The "MRVR message sent" indicator in the MRVA is set if:

(1) The intermediate SP sends an MRVR message to the initiator.

(2) The intermediate SP receives an MRVA message with the "MRVR message sent" indicator set.

C. Initial Actions on Reception of an MRVT Message

9.60 On reception of an MRVT message, the terminator consults its data base of administered MTP routing data to determine if the initiator of the MRVT message is known.

D. Subsequent Actions

9.61 If the initiator is unknown, the test result at the terminator is **failure**, and an MRVA message is sent to the adjacent SP from which the MRVT message was received. This MRVA message indicates "unknown initiator point code" and indicates that an MRVR message was not sent to the initiator. No further MRVT processing is performed in connection with the received message.

9.62 If the initiator is known, the test result at the terminator is **success**, and the following actions are taken:

(1) If the received MRVT message indicates a user request to send an MRVR message to the initiator in case of success, the terminator complies. The MRVR message sent by the terminator indicates **success** and carries the trace found in the received MRVT message. Then, an MRVA message which indicates **success** is sent to the adjacent SP from which the MRVT message was received.

(2) If the received MRVT message does not indicate a user request to send an MRVR message, the terminator does not send an MRVR message. An MRVA message which indicates "success," however, is sent to the adjacent SP from which the MRVT message was received.

Reception of an Unexpected MRVR Message

9.63 An unexpected MRVR message may be received for either of the following reasons:

(a) The MRVR message was generated by some SP as part of an earlier MRVT, but for some reason the MRVR message is delayed in arriving at the initiator.

(b) The MRVR message was generated by an STP in response to the receipt of a signaling message whose Destination Point Code (DPC) in the routing label was not recognized by the MTP data at that STP. Here, the MRVR message shows **unknown terminator point code** and specifies the unrecognized DPC as the unrecognized terminator point code. The MRVR message also contains the PC of the SP that did not recognize the DPC.

9.64 When an SP receives an unexpected MRVR message, the SP reports this through the **REPT MRVR** output message. This output message is received on-site and at the maintenance support system. If the MRVR message shows **unknown**

terminator point code, the output message is accompanied by a minor alarm on the maintenance ROP.

The Definition and Setting of the Timer T1

9.65 The MRVT procedures executed by the initiating and intermediate SPs involve a timer T1, whose expiration signifies the end of the waiting period for the reception and processing of all expected MRVA messages. The value of timer T1 is a function of two user-specified parameter values:

(a) **N** (Maximum Allowed STPs Crossed), which may be specified by a user when the MRVT initialization command **EXC:MRVT** is entered. The default value is 2.

(b) **D** (Delay or Expected Processing Plus Transmission Time of an MRVT message), which can be specified, changed, or verified by a user through the **CHG:MRVT** input message. The allowed range is 8-15 seconds. The default value is 8 seconds. The timer **T1** is calculated as shown in Table 6-L.

Table 6-L. Setting Timer T1

Signaling Point	Function
Initiating Switch	T1 = **D** x (**N** + 1)
Initiating *A-I-Net*® STP	T1 = **D** x **N**
Intermediate *A-I-Net* STP	T1 = **D** x (**N** - # of point codes in trace of received MRVT message)

NOTE:
Timer **T1** at an intermediate SP that is always a positive number; if the number of point codes in the trace is greater than or equal to **N**, an excessive-length route is detected and the test discontinued prior to the setting of **T1**.

MRVT Restrictions

9.66 Restrictions regarding the number of tests that an SP is able to participate in [as the initiator, intermediate (only) SP, or terminator] without any performance impact at any point in time are:

(1) **Test Initiator**: Each SP is limited to no more than five concurrent MRVTs.

(2) **Intermediate SP (only)**: Each is limited to being an intermediate SP for no more than 25 concurrent MRVTs.

(3) **Test Terminator**: There is no limit on the number of tests that an SP should be able to terminate at any point in time.

Network Element Specific Details

A. 1A ESS™ Switch, 4ESS™ Switch, and 5ESS® Switch

(1) If a switch receives an MRVT message with a tested destination point code different from its own point code, the switch ignores the MRVT message.

(2) If a switch receives an unexpected MRVR message (MRVR message not associated with an outstanding MRVT), the switch is requested to send an output message with **MINOR** alarm on a maintenance channel.

B. *A-I-Net* Products STP

(1) Reception of a message for an unknown destination.

When an *A-I-Net* products STP receives any signaling message whose destination point code is not recognized by the MTP, the *A-I-Net* products STP OMAP is required to:

(a) Send an output message with a **MINOR** alarm on the maintenance channel.

(b) Send an MRVR message to the origination point of the received message. The values of the information fields in the MRVR message are:

— Message type: MRVR

— Point code of terminator: the unrecognized destination point code

— MRVT result: unknown terminator point code.

NOTE:
The MRVR message is not associated with any MRVT in progress; it is regarded as an *unexpected MRVR message* by the SP that receives it.

(2) Reception of an *unexpected MRVR message.*

If an *A-I-Net* products STP receives an *unexpected MRVR message*, the *A-I-Net* products STP sends an output message with a **MINOR** alarm on the maintenance channel. The output message is delivered on-site and is made available to 2SCCS.

Network Interconnect Capabilities

9.67 The SS7 standard MRVT test is able to cross any internetwork boundaries and verify message routing paths that may include foreign and nonlocal (that is, conforming to the ANSI T1S1.3 standards) signaling networks.

9.68 The MRVT initially offered by Lucent Technologies and described in this document allows internetwork routes to be tested up to and including the gateways to the nonlocal network. On receipt of an incoming MRVT from the nonlocal network, the normal (MTP and SCCP) screening must have the capability to block the request (by blocking all the OMAP messages from the particular network), if desired. The following parts describe this interaction in more detail.

A. Outgoing MRVT Messages

9.69 For the MRVT feature discussed in this document, an MRVT may be initiated toward a nonlocal terminator (that is, a terminator whose Point Code is in a network different from that of the initiator). However, the MRVT is allowed to progress only up to the gateway into the nonlocal network. Propagation of MRVT messages is stopped at this gateway. The gateway sends an MRVR message to the initiator and an MRVA message to the SP from which the MRVT message was received. Both the MRVR and MRVA messages show a failure condition of **INACCESSIBLE SIGNALING POINT**.

9.70 This mechanism allows internetwork routes to be tested up to and including the local network outgoing gateway. It is not permitted for an MRVT to be initiated from some SP **"X"** towards some SP **"Y"** in another network if the SP **"X"** is a gateway into the other network. This is because the SP or SPs adjacent to SP **"X"**, on the route(s) to SP **"Y"**, are in the other network and thus are considered inaccessible SPs.

B. Incoming MRVT Messages

9.71 For the MRVT feature described in this document, at a local gateway receiving an MRVT message from another network, the MRVT is allowed to progress if and only if both of the following are true.

(a) The incoming MRVT message received at the local network incoming gateway has not been blocked by gateway MTP/SCCP screening. If the local gateway SP is a switch, an MRVT received from a nonlocal network is unconditionally granted since there are no screening capabilities at switch offices.

(b) The type of TCAP encoding (ANSI) in the incoming MRVT message is the same as the type of TCAP encoding used in the local gateway SP.

C. MRVR Messages

9.72 At any SP that is about to send an MRVR message, no message is sent if its destination is to a different network. If the types of TCAP encoding differ, the MRVR message is discarded. When an SP receives an MRVR message from another network, the SP processes the message in the normal manner if the type of TCAP encoding used in the incoming message is the same as the type of TCAP encoding used in the local office.

D. MRVA Messages

9.73 When a local gateway SP receives an MRVT message from another network, the gateway SP eventually returns an acknowledging MRVA message only if the MRVT is allowed to progress at the local gateway SP. If the MRVT is not allowed to progress, no MRVA message is sent by the local gateway SP.

Effect of an Initialization on an In-Progress MRVT

9.74 An MRVT may be in progress when an initialization occurs. The basic strategy on initializations is to recover gracefully without concern for an in-progress MRVT.

9.75 For a CNI level 1 initialization, the current MRVT status is not changed. It is quite likely, however, that MRVA/MRVR messages are lost. This can result in misleading output messages and an incorrect diagnosis.

9.76 For a CNI level 2 initialization, 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 can also generate misleading output messages.

9.77 For CNI levels 3 and 4 initializations, it is extremely unlikely to receive a "straggler" MRVA or MRVR message.

9.78 The file that contains Delay Parameter D is read by OMAP on CNI levels 2, 3, and 4 initializations; the value of this parameter is not lost.

9.79 Personnel initiating the MRVT command should be aware of any initialization levels occurring during the MRVT so they may rerun the test. They should not be misled by MRVT output messages received after the initialization but before a new MRVT initiation (although an MRVR message received with an **UNKNOWN TERMINATOR POINT CODE** indication is legitimate, that is, it is an unexpected MRVR).

MRVT Example Message Flows

9.80 All of the messages follow normal MTP routing. The MRVT and MRVA messages are always routed to an adjacent SP and normally use the direct linkset if it is available. If the direct linkset is unavailable, the MTP routes *via* an adjacent STP. When the messages are MTP-routed *via* an STP, there is no OMAP processing at those MTP-intermediate STPs. The MRVT does not change or interfere in any way with normal MTP routing.

A. Switch Routing Through Local STPs to Adjacent Switch

9.81 As shown in Figure 6-6, the MRVT initiator is switch (7) and the terminator is switch at (6). The initiator sends MRVTs (7-4) and (7-5). They in turn propagate MRVTs (7-4-6) and (7-5-6). On receipt of the MRVT messages, terminator (6) consults its data base of administered MTP routing data to determine if the named initiator is known. Terminator (6) recognizes initiator (7).

9.82 The test result at switch (6) is **success**. Switch (6) sends an MRVA message to each of the adjacent SPs that sent it an MRVT message; in this case, STPs (4) and (5). The MRVA message indicates **success** and that an MRVR message was not sent to the initiator (this is specified in the initiation command).

9.83 The intermediate SPs (4) and (5) receive an MRVA from (6). They in turn send an MRVA message back to the initiator (7). This MRVA is formatted to indicate **success**.

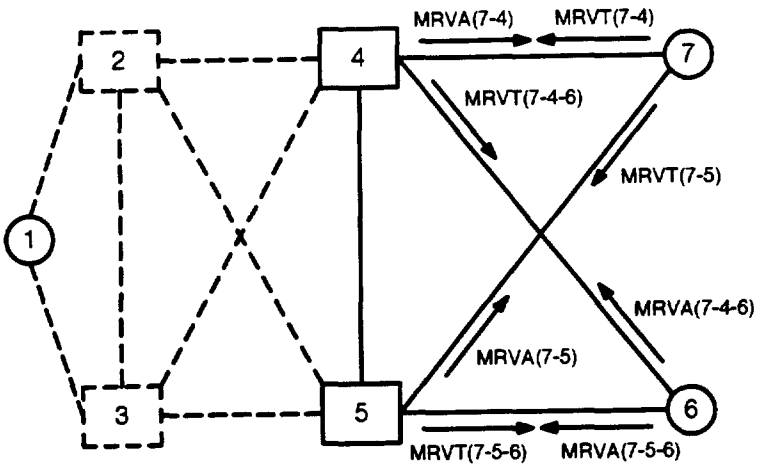
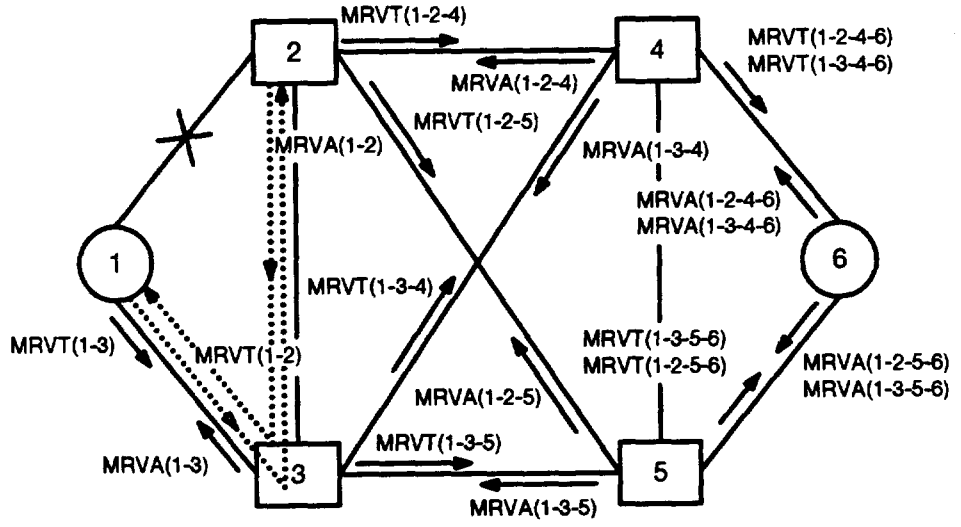


Figure 6-6. Example Where Switch Routes Through Local STPs to Adjacent Switch

B. A-Linkset Failure

9.84 As shown in Figure 6-7, the MRVT initiator is switch (1) and the terminator is switch (6). Due to the failure of an A-linkset between STP (1) and STP (2), the MRVT message cannot be transmitted over the direct link to STP (2). Switch (1) now has to transmit the MRVT message over an alternate MTP path.

9.85 In this scenario, the A-link (1)-(3) and the C-link (3)-(2) are used. For this message, STP (3) acts only as a simple MTP signal transfer point and not as an MRVT intermediate SP; only the MTP protocol layers are involved in the process. Therefore, the trace delivered by MRVT (1-2-4) to MRVT processing at STP (4) contains only the STP (2). In all other respects, MRVT (1-2-4) shows no evidence to MRVT processing at STP (4) of being generated by STP (3).



Note: Alternate MTP routing (dotted line) between #1 and #2 via #3 does not change test result.

Figure 6-7. Example of MRVT Message Routing Under A-Linkset Failure

C. B-Linkset Failure

9.86 As shown in Figure 6-8, the MRVT initiator is switch (1) and the terminator is switch (6). The STP (2) receives MRVT (1-2) from the initiator, then formats MRVT (1-2-4) for destination STP (4). Due to the failure of a linkset between (2) and (4), the MRVT message cannot be transmitted over the direct link to STP (4). The STP (2) now has to transmit the MRVT message over an alternate MTP path.

9.87 In this scenario, the B-link (2)-(5) and the C-link (5)-(4) are used. For this message, STP (5) acts only as a simple MTP signal transfer point and not as an MRVT intermediate SP; only the MTP protocol layers are involved in the process. Therefore, the trace delivered by MRVT (1-2-4) to MRVT processing at STP (4) contains only the STP (2). In all other respects, MRVT (1-2-4) shows no evidence to MRVT processing at STP (4) of being generated by STP (5). At the same time, STP (5) performs MRVT processing on receipt of MRVT (1-2-5), which also arrived at (5) over B-link (2)-(5). Evidence of this MRVT processing is contained in MRVT (1-2-5-6), which STP (5) formats then transmits to the terminator (6).

9.88 The DPC of an MRVR message is the MRVT initiator, which is not always adjacent to the SP that transmits the MRVR. As previously mentioned, the MRVR message propagates through MTP routing along any available route, and the usual MTP mechanisms that compensate for any linkset failures still apply.

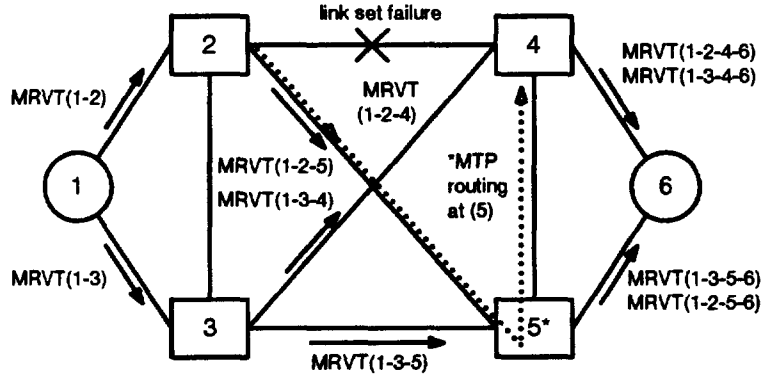


Figure 6-8. Example of MRVT Message Routing Under B-Linkset Failure

D. Terminator Does Not Recognize Originator

9.89 As shown in Figure 6-9, the MRVT initiator is switch (1) and the terminator is switch (6). On receipt of the MRVT message, terminator (6) consults its data base of administered MTP routing data to determine if the named initiator is known. Terminator (6) does not recognize initiator (1).

The test result at switch (6) is failure. Switch (6) sends an MRVA message to each of the adjacent SPs that sent it an MRVT message [that is, STPs (4) and (5)]. The MRVA message indicates **unknown initiator point code** and the fact that an MRVR message was not sent to the initiator. No further processing of the MRVT is performed at switch (6).

The intermediate SPs (4) and (5) receive an MRVA from switch (6). They in turn send an MRVR message back to the initiator (1). This MRVR is formatted to indicate **unknown initiator point code** and contains the point code of the SP that sent the MRVA message.

NOTE:
A separate MRVR message is sent for every received MRVA message of this type. Should the intermediate SP receive an MRVA message which indicates **unknown initiator point code** and that an MRVR message was sent, then no MRVR message is sent in response to the received MRVA message.

The result of the test is **failure**. This is because none of the conditions for **success** or **partial success** are met.

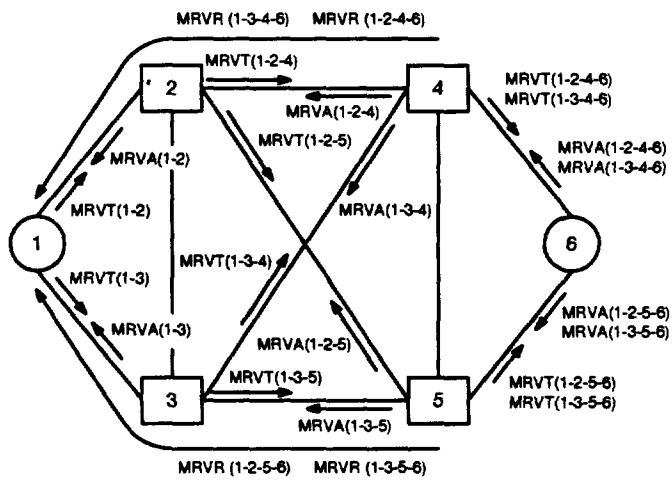


Figure 6-9. Example When Terminator Does Not Recognize Originator

E. Intermediate Signaling Point Does Not Recognize Originator

9.90 As shown in Figure 6-10, the MRVT initiator is switch (1) and the terminator is switch (6). On receipt of the MRVT messages (1-2-4) and (1-3-4), STP (4) consults its data base of administrable MTP routing data to determine if the named initiator is known. The STP (4) does not recognize initiator (1). The STP (4) sends an MRVA message to each of the adjacent SPs that sent it an MRVT message [that is, STPs (2) and (4)]. The MRVA message indicates **unknown initiator point code** and that an MRVR message was not sent to the initiator. No further processing of the MRVT is performed at (4).

9.91 The intermediate SPs (2) and (3) receive an MRVA from STP (4). They in turn send an MRVR message back to the initiator (1). This MRVR is formatted to indicate **unknown initiator point code** and contains the point code of the SP that sent the MRVA message.

9.92 The result of this test is **partial success** since at least one expected MRVA message was received by initiator (1). In this scenario, terminator (6) was able to receive MRVT messages (1-3-5-6) and (1-2-5-6).

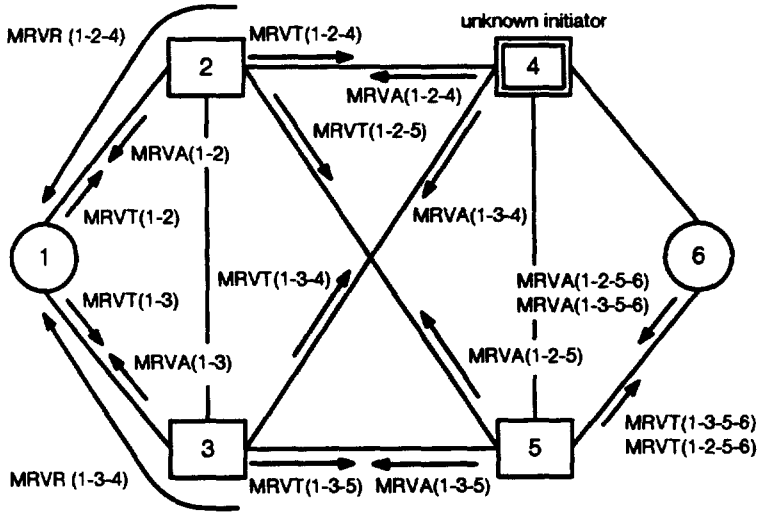


Figure 6-10. Example When Intermediate SP Does Not Recognize Originator

F. Detection of a Routing Loop

9.93 As shown in Figure 6-11, switch (1) initiates an MRVT to the switch (6). Incorrect routing data at STP (2) causes MRVT (1-2-7) to be sent to STP (7), which is in a different level than STPs (2), (3), (4), and (5). The STP (7) sends an MRVT message to STP (4). The STP (4) has incorrect routing data which indicates that STP (2) is the next valid loop toward the switch (6). The STP (4) finds that STP (2) is already listed in the trace of the MRVT message received from STP (7). A routing loop has now been detected. The STP (4) notifies the MRVT initiator of the *detected routing loop* via the MRVR (1-2-7-4). This MRVR message records the identities of the SPs in the loop.

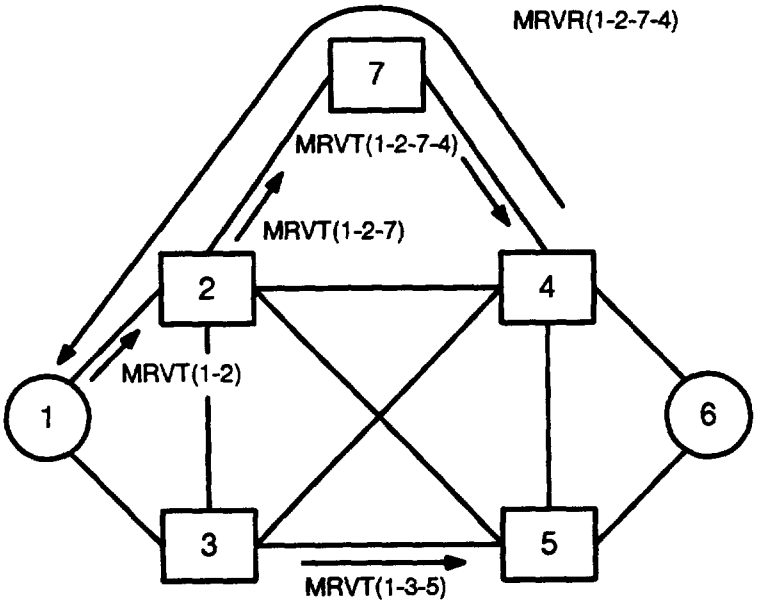


Figure 6-11. Example When Routing Loop Detected

10. Signaling Connection Control Part Routing Verification Test

Overview of SRVT

10.01 This section describes the Signaling Connection Control Part (SCCP) Routing Verification Test (SRVT) feature.

10.02 The SRVT is a CCITT (Q.795) as well as an American National Standards Institute (ANSI) standard Operations, Maintenance, and Administration Part (OMAP) procedure. The purpose of OMAP is to provide an SS7 protocol-defined set of procedures that are used for operation, maintenance, and administration of SS7 signaling networks.

10.03 To provide SRVT, OMAP uses the services of the Transaction Capabilities Application Part (TCAP). The SRVT software for Local Exchange Carrier (LEC) customers follows the ANSI TCAP protocol.

10.04 The SRVT verifies routes only at the SCCP level. The present version of SRVT provides for intranetwork operations only. Protocol enhancements via the standards process (CCITT and ANSI) are necessary for future internetwork application of the SRVT.

10.05 Lucent Technologies products not equipped with the SRVT feature will discard any SRVT message that is received without any harm to the network.

10.06 Table 6-M identifies the various Lucent Technologies products that are available with SRVT.

Table 6-M. SRVT Generic Software Releases

1A ESS™ Switch APS	4ESS™ Switch APS	5ESS® Switch	*A-I-Net*® STP
1AP3E & later	4AP10 & later	5E6 & later	Release 0 & later

Purpose of SRVT

10.07 The SRVT can be used to verify the installation of GTT data and therefore aid in preventing translation errors from entering the network. The test can also be initiated when a problem is suspected in GTT as the result of network surveillance indications or as the result of a customer trouble report. The test can be used to troubleshoot and isolate the problem and to verify the repair following the corrective action taken by the responsible center.

10.08 The SRVT can detect the following kinds of problems existing in an SS7 network:

- SCCP routing loops
- Excessively long routes
- Inaccurate routing in both directions on SCCP routes
- Unknown destinations
- Inaccurate, incomplete, or inconsistent GTT data.

Description of SRVT

10.09 The SRVT provides a mechanism for testing the SCCP GTT data for accuracy, completeness, and consistency in the SS7 network and to sectionalize any routing problems discovered in the network. The SRVT checks the static data base SCCP routing data for a tested GT. Static data base routing data is different from dynamic routing data, which is the data that determines the routing in effect at a given time. The dynamic routing data is determined by the static routing data and the history of network outages and recoveries. The SRVT will not check dynamic routing data.

10.10 The SRVT performs this testing by simulating the process involved in query/response transactions which take place between signaling points that are involved.

10.11 The SRVT procedure uses three OMAP test messages:

(1) SCCP Routing Verification Test (SRVT) Message

(2) SCCP Routing Verification Acknowledgement (SRVA) Message

(3) SCCP Routing Verification Result (SRVR) Message.

NOTE:
In this section, the acronym SRVT when shown alone refers to the test itself. The phrase SRVT message refers to the SRVT test message.

10.12 The SRVT message serves three different roles:

(1) The Request form of the message is sent by the test initiating Signaling Point (SP) to request a GTT. 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 another ITSP or a Final Translation Signaling Point (FTSP).

(2) The Verify form of the message is sent by the FTSP to the destination SP(s).

(3) The Compare form of the SRVT message is sent by a TSP to its mate TSP to compare results of duplex translation at the mated pair of STPs.

10.13 The SRVA message is sent in the backward direction on a hop by hop basis, that is, the recipient of the SRVT message sends an SRVA message to the sender of the SRVT message, informing the sender of the success of the test and in case of failure, the cause of the failure.

10.14 The SRVR message is sent in the backward direction by the destination SP or an intermediate 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 to another SP if identifying a failure. This is referred to as route trace information. In addition, the message contains the results of the test whether success or failure. In case of failure, the cause of the failure is identified.

Operational Description of the SRVT Process

10.15 This section describes the common operations that occur during an SRVT, that is, operations that occur regardless of whether the initiating SP or destination SP is a 1A ESS Switch, 4ESS Switch, 5ESS Switch, or *A-I-Net* products STP.

SRVT Procedure Description

10.16 The SRVT procedure checks all possible SCCP routes. The initiating SP sends one SRVT message for each point code received for the translation type checked. If the point code is an Alias Point Code, only one SRVT is sent.

10.17 With respect to the *A-I-Net* products STP network, if one point code called an Alias represents a mated pair of *A-I-Net* products STPs that can translate a given Global Title, then the initiating SP needs to know only that one point code. An Alias Point Code is a point code identification assigned to multiple TSPs, all of which can perform the translation for a given Global Title.

10.18 Each TSP sends one SRVT message to each of up to two SPs resulting from the translation. The SPs may be TSPs or tested destinations.

10.19 If an SP receives an SRVA, SRVR, or SRVT message containing information other than that specified in the part "Test and Acknowledgement Messages for the SRVT," it is ignored.

10.20 Whenever an SP detects an error it stops the test except when responding to the SRVT Compare message from the mate TSP, that is, the mate performing the Comparison does not stop the test.

10.21 System Management Application Process (SMAP) is performed at the SP where an error is detected. The results will be printed out only at the initiating SP (at the local terminal or via the OS at the remote location), and the report will separately list each SRVR message but integrate the results of all SRVA messages.

10.22 In the case that no error is detected as the test progressively moves forward and reaches the tested destination, the test stops at the tested destination.

10.23 When the test is stopped and the expected SRVR messages and the SRVA message(s) are received at the initiating SP, the results are reported to the initiator.

10.24 If, in the course of responding to an SRVT message, a signaling point determines that it cannot send an SRVA message, then no further action is required of the signaling point.

SRVT Initiation

A. SRVT Initiation Capability

10.25 All the network elements (1A ESS Switch, 4ESS Switch, 5ESS Switch, and *A-I-Net* products STP) are capable of initiating the SRVT (a) locally via an Administrative terminal or Maintenance terminal and (b) remotely via one or more Operation Support Systems (OSs). All network elements are also required to respond to the supplemental command (OP:TPC) specified in "Input Messages for the SRVT" in this chapter if this command is received from any of the on site or remote interfaces from which the initiation command can be received. For additional information, refer to the appropriate system I/O manual for message details.

B. Initiating SP Requirements

Checks Performed Before Initiation

10.26 The initiating SP will check for and report out of range parameters in the initiation command. The identity of the parameter(s) found to be in error will be included in the report.

10.27 If no TPC is specified in the initiation command and the initiating SP does not know how to obtain GTT for the specified GT, the SP responds with "UNABLE TO DERIVE TPC." If a TPC is specified in the initiation command, or the SP knows where to send the SRVT message to perform the GTT for the specified GT, the initiating SP will perform the following checks before initiating the SRVT procedure.

(1) The initiating SP will check to verify that the GT in the initiation command is not already under test. If the GT is already under test, it reports the "Local Condition" error. A suffix letter in the error code identifies the local condition. Refer to "Output Messages (Reports) for the SRVT."

(2) The initiator checks to see if the threshold for simultaneous SRVT tests at that SP has already reached its limit value of 5. If the threshold has already been reached, the request to initiate the SRVT is rejected and the initiator is provided with the "Local Condition" error response. A suffix letter in the error code identifies the local condition.

(3) If the test cannot be initiated due to processor overload, the SP rejects the SRVT request and provides the "Local Condition" error response. A suffix letter in the error code identifies this local condition.

(4) If the SRVT message cannot be forwarded to the TSP or the tested destination because of network blockage or congestion, the user is given a response identifying "Route Inaccessible" error condition. If the message is destined for an SP that is across the network boundary, not SS7 equipped, subsystem prohibited, or receiving unit data service message, the user is also given a "Route Inaccessible" response. A suffix letter in the error code identifies the route inaccessible condition.

(5) The initiator will NOT check whether a TPC specified by the user in the initiation command is in fact one of the TPCs in its SCCP routing data. Assuming the foregoing checks (items A-D) pass and if the TPC is a point code (true or Alias) which the initiator recognizes as belonging to itself, the initiator will initiate an SRVT as if no TPC had been specified. If the TPC is not a point code (true or Alias) which the initiator recognizes as belonging to itself, the initiator will send an SRVT Request message to the TPC specified in the initiation command.

10.28 The initiating SP sends one SRVT Request or Verify form message to each distinct point code returned by the Translation Result Interface except when a TPC is specified, in which case exactly one SRVT message is sent.

Translation Signaling Points

A. Translation Signaling Point Capability

10.29 In addition to acting as an initiating SP, the *A-I-Net* products STP will also have the capability to act as a TSP. The *A-I-Net* products STPs are always deployed as mated signaling points with **C-links** connecting each mated pair. In its role as a TSP the *A-I-Net* products STP will also provide the duplex translation function.

Intermediate Translation Signaling Point

10.30 The function of the Intermediate Translation Signaling Point (ITSP) can be performed by the *A-I-Net* products STP. The ITSP performs an intermediate Global Title translation on the GT contained in the SRVT Request form message. It forwards an SRVT Request message to each distinct point code in the Global Title translation data. The resulting message(s) leaving the ITSP has its Destination Point Code (DPC) changed to that of the next TSP(s) and the Originating Point Code (OPC) changed to that of the ITSP. However, the tested GT in the SRVT message is not changed. The SSN parameter is not in the TCAP portion of the message. The SRVT message that leaves the ITSP is still the Request form of the SRVT message. The *A-I-Net* products STP acting as an ITSP is always duplexed and is required to send a Compare message to its mate to validate the consistency of the translation.

Final Translation Signaling Point

10.31 The function of the Final Translation Signaling Point (FTSP) is performed by the *A-I-Net* products STP. The FTSP performs the final translation on the GT contained in the initiation command or the SRVT message it receives. Final translation implies that the GT is translated to PPC+SSN (with the option to also include an SPC+SSN). The DPC in the message is that of the PC resulting from the translation at the FTSP. This message is the Verify form of the SRVT message. It differs from the Request form in that this message contains the SSN whereas the message leaving an ITSP does not. The *A-I-Net* products STP acting as an FTSP is always duplexed and is required to send a Compare message to its mate to validate the consistency of the translation.

B. Excessive Length Detection at TSP

10.32 For detecting excessive length route, a TSP must determine the count **C** of the crossed TSPs from the list of point codes contained in the trace. The count **C** is compared with the threshold parameter **N** contained in the message for determination of whether or not an excessive length route has been detected.

10.33 For each mated *A-I-Net* products STP acting as a TSP, the trace contains two point codes. The count **C** is determined by dividing the number of point codes in the trace by 2. If the result is not a whole number, it is rounded up to the next whole number. An excessive length route is detected if **C** is greater than or equal to **N**.

C. Duplex Translation

10.34 The *A-I-Net* products STP is deployed in mated pairs. It is mandatory for an *A-I-Net* products STP with SCCP GTT function (irrespective of whether it is acting as an ITSP or FTSP) to send a Compare form of the SRVT message so that the results of the translation can be compared with those results from the translation at the mate *A-I-Net* products STP. If the results of the translation do not match, or if the mate does not have the translation, the errors reported via the SRVA message are identified as stated below.

(a) Incorrect translation for the PPC+SSN at the FTSP

(b) Incorrect translation for the PPC+SSN at the FTSP

(c) Incorrect translation for the Intermediate TSP.

Tested Destinations

A. Signaling Points Acting As Tested Destinations

10.35 The *A-I-Net* products STP, 1A ESS Switch, 4ESS Switch, and 5ESS Switch have the capability to perform the functions required of the tested destination. The SCPs are deployed as mated pairs or on a nonmated pair basis.

10.36 The tested destination function in the 1A ESS Switch, the 4ESS Switch, and the 5ESS Switch is provided on a nonmated (nonduplicated) basis.

B. Tested Destination

10.37 After receiving the SRVT message, the test destination performs the following checks.

(1) The test destination checks to ensure that the SRVT message it has received is of Verify form. If the message is not in the Verify form, it reports the error "Wrong SP."

(2) It compares its own point code (DPC in the routing label) with the PPC and with the SPC (if present). If the DPC matches with neither the PPC nor the SPC, the destination reports the error "Wrong SP."

10.38 Primary Point. If the DPC = PPC, the recipient destination is a primary point for the GT. The destination then performs the following checks.

(1) The SSN associated with the PPC is valid.

(2) It serves the GT in the context of the SSN.

(3) It serves the GT as primary, that is, the PPC+SSN received in the message matches with the PPC+SSN associated with the GT at the destination.

(4) The identity of the secondary (SPC+SSN) received in the message matches with the SPC+SSN associated with the GT at the destination.

(5) If all of the applicable checks are successful, the destination serves the GT; otherwise, an error is reported.

Secondary Point. If DPC = SPC, the recipient destination is a secondary point for the GT. The destination performs checks similar to those stated under "Primary Point Requirements."

DPC matches with PPC as well as SPC. The destination performs the checks stated above until it detects an error. The first error detected is reported.

SCP as Test Destination. To serve as a test destination, the SCP will verify the full complement of GT digits within the context of the application.

C. Switch or Nonmated Destinations

10.39 The switch or nonmated SCP performs the checks listed under "*Signaling Points Acting As Tested Destinations.*"

10.40 The switch or nonmated SCP will not have an SPC+SSN associated with GT at the destination. Therefore, the absence of SPC+SSN is normal if DPC=PPC in the SRVT message, and its presence is invalid. If SPC+SSN is present, the reported error is "Secondary Destination Not Recognized."

If the switch or nonmated SCP receives a message such that DPC = SPC, it is invalid and reported as the error "Not Secondary Destination."

D. Verification of Global Title Digits

10.41 In order to verify the Global Title digits within the context of the SSN, the SRVT software has a standard interface to a defined SRVT application code. The interface passes the SSN and the GT digits to the SRVT application code. This application code determines whether the GT digits are valid for the specified SSN and provides the results of its determination to the SRVT software at the interface.

The GT digits for the switch are assumed to be a telephone directory number having the format NPA NXX XXXX and the application will verify at least the first six digits of the directory number. If a new application is ever implemented that does not use the directory numbers for GTT, the SRVT application process will be updated to accommodate the new type of GT digits. Since directory numbers are the most likely GT digits the switches will receive, the default treatment for a new application will be to assume the digits are a directory number.

RVM Messages

RVM Message Capabilities for Network Elements

10.42 The SRVT procedure uses three OMAP messages:

(1) The SCCP Routing Verification Test Message (SRVT)

(2) The SCCP Routing Verification Acknowledgement Message (SRVA)

(3) The SCCP Routing Verification Result Message (SRVR).

All the network elements have the capability of generating and responding to these messages.

Additional Clarifications and Requirements

A. Results Output to the Initiator Only

10.43 The results of the test are printed out only at the initiating SP's local terminal or via the OS at the remote location, where SMAP is informed of any error. The printout report lists each SRVA and SRVR message separately that was 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 that are listed.

10.44 When the SRVT is initiated at the TSP, no SRVR and SRVA messages are sent from the TSP to the initiating SP, since the TSP itself is the initiating SP. However, the results will be printed out in the same format as when the TSP function is remote. If a "Local Condition" or "Inaccessible Signaling Point" error is detected at the initiating SP, a suffix letter in the error code is required to identify the cause of the error.

B. C-Link Failure

10.45 If, in the course of responding to an SRVT message, an *A-I-Net* products STP finds its mate inaccessible for the routing of the Compare message, the test continues and the forward progress of the test is not stopped. The *A-I-Net* products STP times out and then sends SRVR and SRVA messages, and the error reported is "Timer Expired."

C. Response to SRVT from an SP with No SRVT Capability

10.46 If the SRVT is sent to an SP which does not have the SRVT capability, there is no guarantee that the initiating SP will get any meaningful response. Any response is ignored unless it is a Unitdata Service Message. The initiating SP will time out and provide the results to the initiator.

D. SRVT Messages Across the Network Boundary

10.47 The *A-I-Net* products STP acting as a TSP is required to detect an SRVT message destined to go across the network boundary and will report this as a "Route Inaccessibility" error.

E. Use of True Versus Alias Point Codes

10.48 Only the true point codes (not alias or capability codes) will be used for the DPC of an SRVT Compare message; the OPC of an SRVT, SRVA, or SRVR message; and for each trace entry in an SRVT or SRVR message.

F. Characteristic of Data Checked

10.49 The SRVT will check the master copy of administered (Static Data base) translation data.

G. Routing of SRVR Messages

10.50 The SRVR message is routed to the Initiator using the initiator's point code if the MTP Backward Routing Required Indicator is set and the initiator's point code is recognized. If the MTP Backward Routing Required Indicator is not set, then routing is based on the Initiator's GT. If the MTP Backward Routing Indicator is not set or if the MTP Backward Routing Indicator is set but the initiator's point code is not recognized, the reported error is "Unknown Initiator."

Operating System Capabilities

10.51 Operation Systems (OS) and devices capable of initiating SRVT tests, receiving test results, and analyzing the results are listed below.

(a) Number 2 Switching Control Center System (2SCCS) impacts 1A ESS Switch, 4ESS Switch, 5ESS Switch, *A-I-Net* products STP, and *A-I-Net* products SCP.

(b) Administrative CRT (ACRT)/Maintenance CRT (MCRT) impacts 1A ESS Switch, 4ESS Switch, 5ESS Switch, *A-I-Net* products STP, and *A-I-Net* products SCP.

Operational Scenarios

10.52 This section illustrates the SRVT process by creating network scenarios and describing SRVT message flows.

10.53 Each scenario is illustrated by a figure and accompanying information as to the identity of the initiating SP, the TSP(s), the tested destination, the network condition, and the test result. The network condition typically represents an error condition being detected or ignored by the SRVT in its role to verify the accuracy of the GTT. The test results are also listed for each scenario.

A. Network Normal, Indication Success

10.54 Figure 6-12 represents a normal network condition. No error has been detected and the destination has declared success and reported it in the SRVR message. The SRVR message contains a trace of the SCCP translation points. The only translation points on the route are **B** and **C**. The SRVR message is MTP Routed. It contains point code identification of **B** and **C**. Success via the SRVA message means that no errors are being reported in the message. The SRVR message is MTP routed because it was requested to be MTP routed.

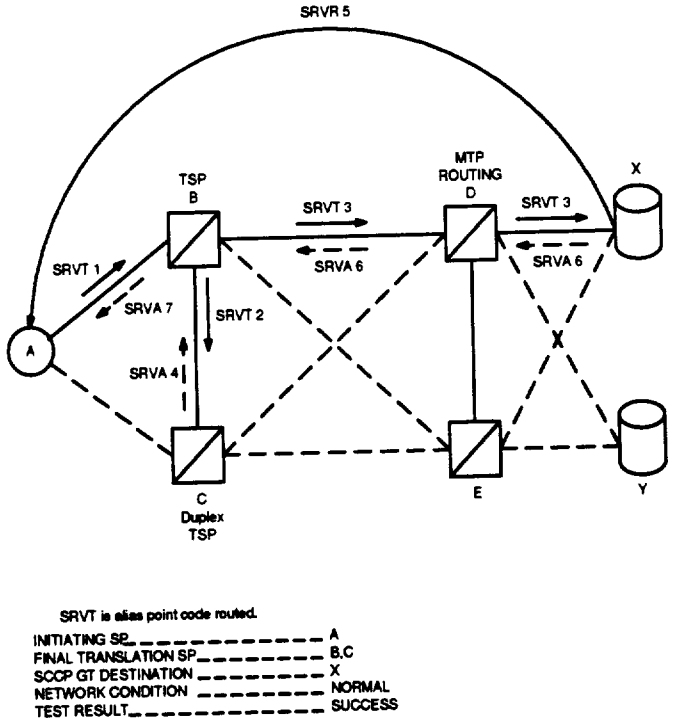


Figure 6-12. Network Normal, Indication Success

B. SCCP Routing Loop

10.55 The SCCP routing loop is caused by an error at the FTSP as shown in Figure 6-13. The error is present in both TSPs **D** and **E**. The FTSP **C** in fact is saying that the final translation resides at **H**. The GTT at **H** (correctly) identifies that the SRVT message should be forwarded to **E**. **H** examines the list of crossed TSPs and learns that the point code of **E** is already on the list. An SCCP loop will result if **H** forwarded the SRVT message to **E**. Therefore, **H** does not forward the SRVT message to **E**. It reports the loop condition via the SRVR and SRVA messages. The SRVR message contains the point codes of **B,C; D,E; H, I.**

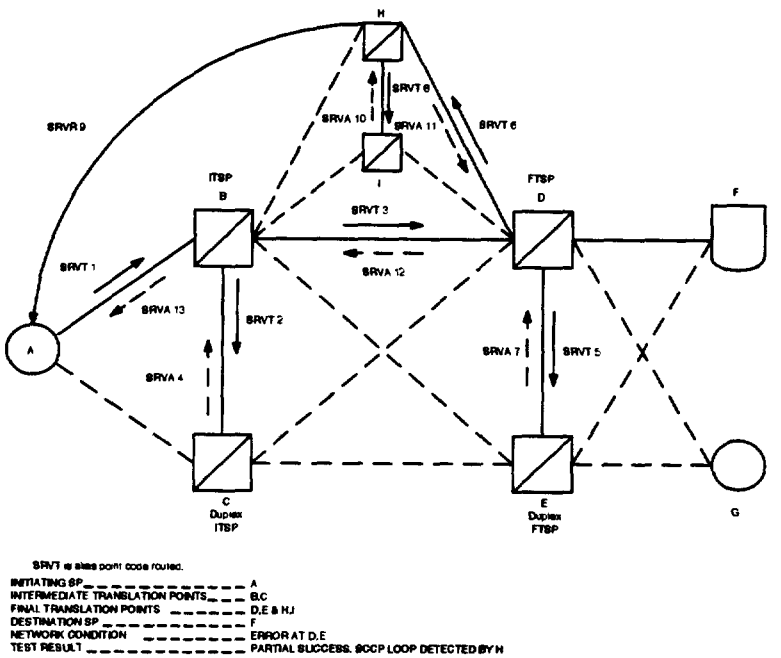


Figure 6-13. Detection of SCCP Routing Loop

C. MTP Routing Loop

10.56 The MTP routing loop is caused by a routing error (Figure 6-14) at **D** and **E**. **D** misroutes the SRVT message to **H**. **H** routes it to **E**. **E** routes to **D**, and so on. The message is MTP routed. **D** and **E** are not the SCCP translation points. The error is not detected. **B** times out waiting for SRVA and then sends a "Timer Expired" indication via the SRVA message to **A**. **B** identifies **F** as the SP (by point code in the SRVR message) which did not send the SRVA message.

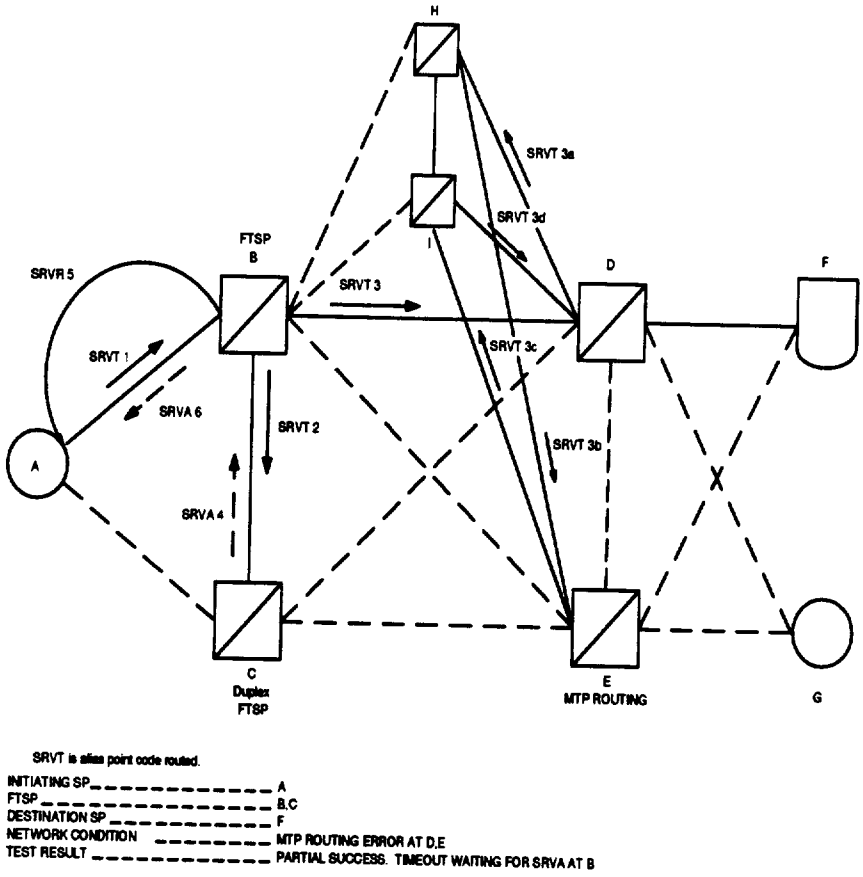


Figure 6-14. MTP Routing Loop

D. Excessive Length SCCP Route

10.57 The excessive length SCCP route problem is caused by an error in SCCP routing at **B** (Figure 6-15). **B** routes the SRVT message to **H** (absent the error, it should have routed to **D**). Prior to sending the SRVT message forward, **H** examines the list of crossed TSPs. The list contains two point codes, that is, of **B** and **C**. **H** determines that the count **C** is less than the value of parameter **N**, so it sends an SRVT message forward to **D** after adding its own point code and the code of its mate. The excessive length route is detected at **D** when it determines that **C = N = 2**. The error is reported by SRVR 9 message and SRVA 13 message (via SRVA 11 message and SRVA 12 message).

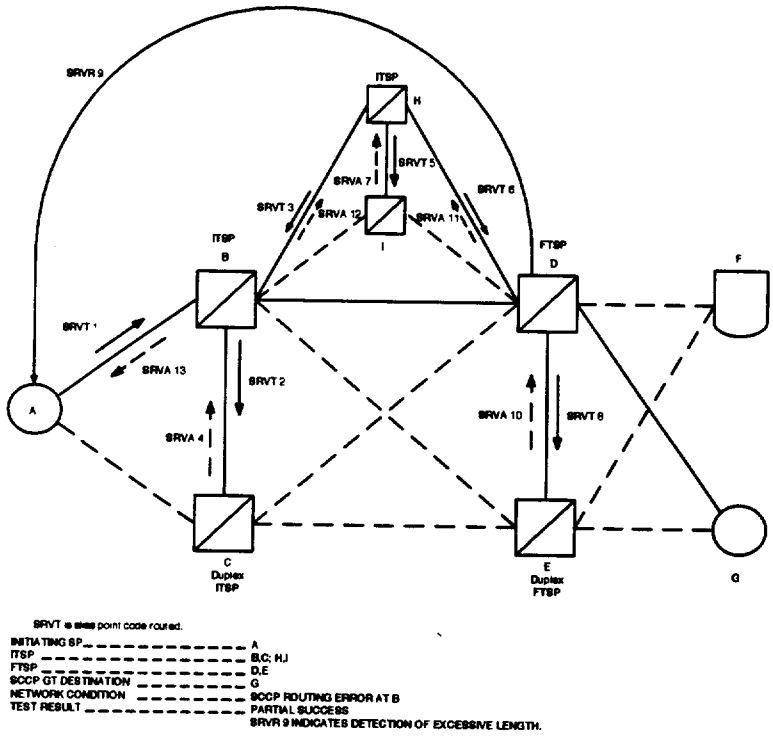


Figure 6-15. Detection of Excessive Length SCCP Route

E. MTP Route Excessive Length

10.58 The excessive length problem is caused by an MTP routing error at **B** (Figure 6-16). After final translation at **B**, the SRVT message is forwarded to **H** (absent the routing error, the SRVT message should have been forwarded to **D** or **E**). **H** correctly MTP routes the SRVT message to **D**. **D** MTP routes it to **G**. **G** sends back an SRVR message to the initiator indicating success. **B** receives an SRVA message and reports success (no errors) in the SRVA message to the initiator. The MTP routing error remains undetected.

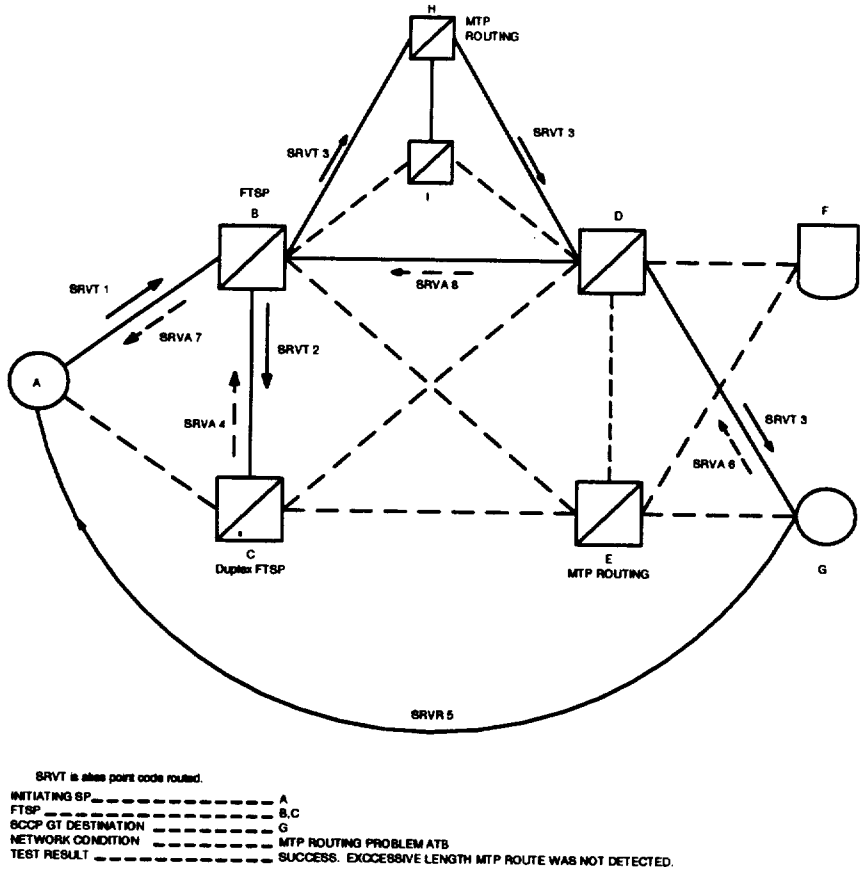


Figure 6-16. SRVT Does Not Detect Excessive Length, MTP Route

F. No GT Translation

10.59 In this scenario, **B** (Figure 6-17) receives the SRVT message and determines that there is no translation for the GT received in the message. It reports the error by responding with SRVR and SRVA messages as shown.

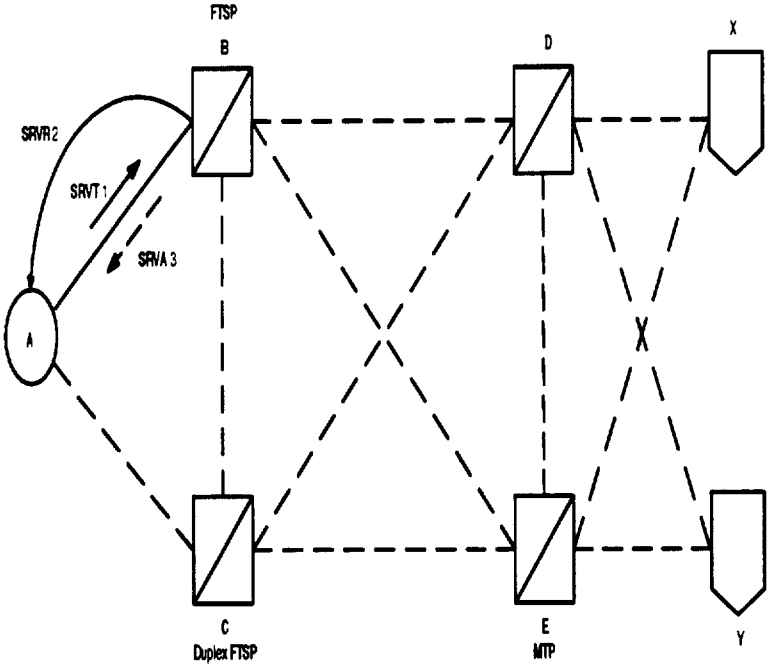


Figure 6-17. No GT Translation at B

G. Inaccessible Signaling Point

10.60 Referring to Figure 6-18, the route inaccessibility condition is detected at **D**. The reason for inaccessibility is that **F** is not accessible using SS7 protocol. The SP which is inaccessible (**F**) is identified by point code in the SRVR message.

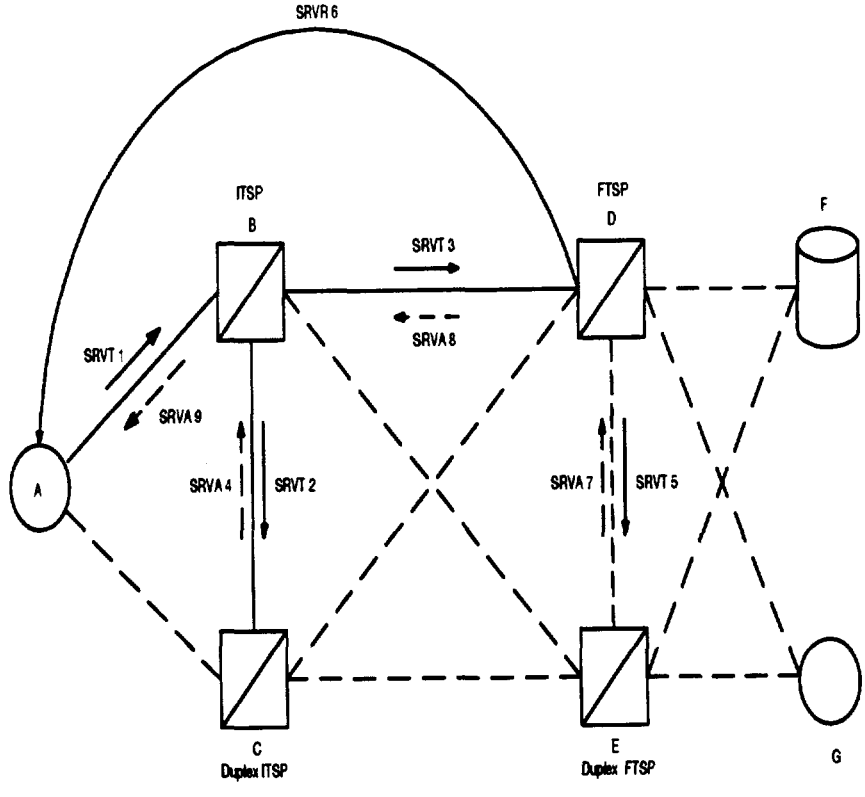


Figure 6-18. Inaccessible Signaling Point

H. Test Cannot Be Run Due to Local Conditions

10.61 Referring to Figure 6-19, on receiving the SRVT Request form of the message, **C** determines that it cannot run this test because the number of SRVT tests already running is 25. It sends the SRVR and SRVA message to inform the initiator of the "Local Condition" prohibiting the continuation of the test.

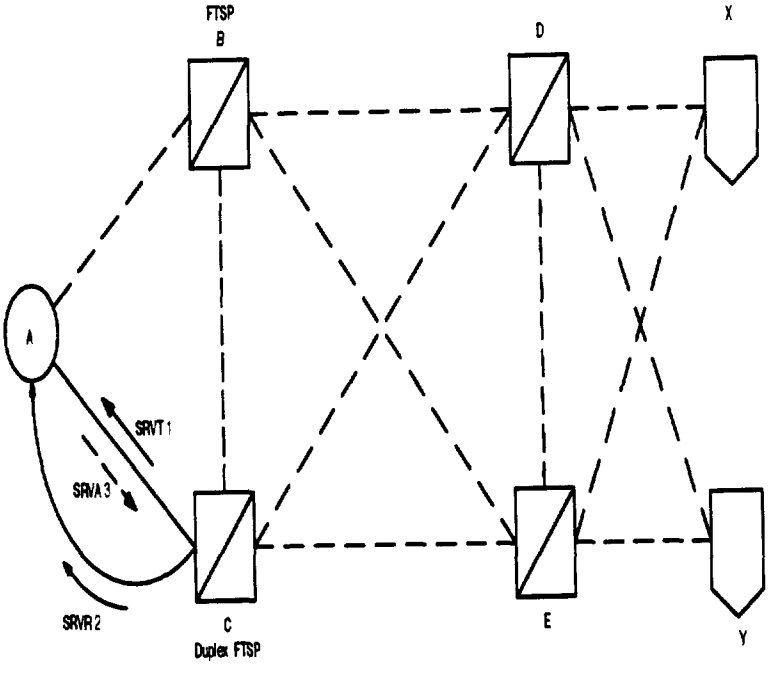


Figure 6-19. Test Cannot Proceed Because of Local Conditions

I. Unknown Initiating Signaling Point

10.62 The destination **X** determines that it does not recognize the initiator's point code. It cannot send an SRVR message. It conveys the unknown initiator information via the SRVA message to **B** (Figure 6-20). **B** sends an SRVR and an SRVA message to **A**. The unknown initiator condition is identified in the SRVR and SRVA messages. The SRVR message also contains the point code identification of X, which does not recognize the initiator.

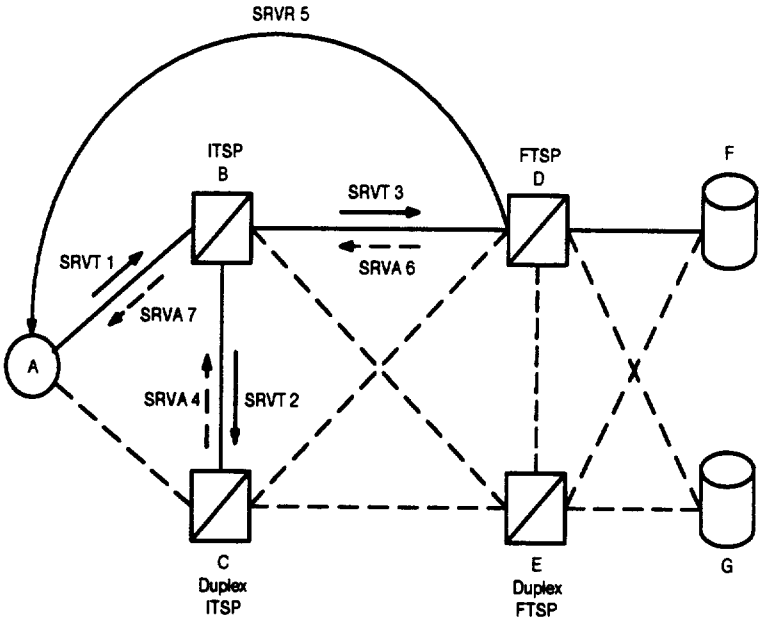
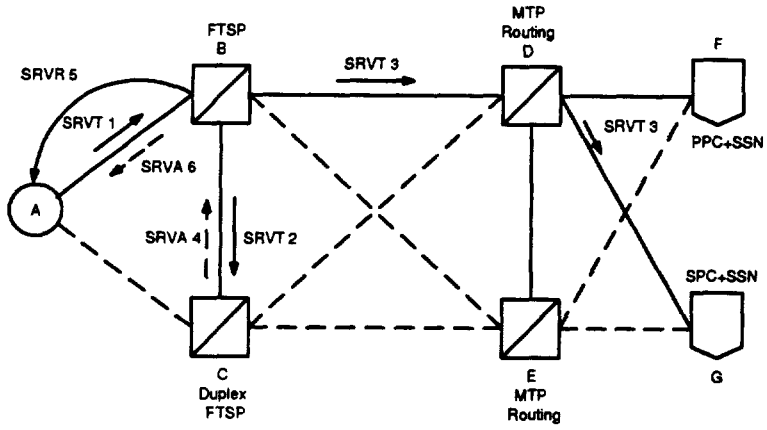


Figure 6-20. Unknown Initiator

J. Time Expired

10.63 Referring to Figure 6-21, following the final translation for the GT at **B**, an SRVT Verify form of the message is MTP routed to **F**. Because of the MTP routing error at **D**, the message is misdelivered to **G**. **G** should have sent an SRVR message and an SRVA message, but because of congestion it is unable to send an SRVA message or SRVR message. The timer expires at **B** waiting for an SRVA message. **B** sends SRVR and SRVA messages to **A**. The SP which did not send an SRVA message is identified in the SRVR message as **F** (although **F** never received an SRVT message). The scenario points out that in case of MTP routing errors, one can get a wrong indication, and it is necessary to run an MRVT test to identify MTP routing errors.



SRVT is alias point code routed.

INITIATING SP	A
FINAL TRANSLATION	B,C
SCCP GT DESTINATION	F (PPC+SSN)
NETWORK CONDITION	MTP ROUTING ERROR AT D SVRVT SENT TO G WHICH HAS PROCESSING DIFFICULTIES.
TEST RESULT	PARTIAL SUCCESS. TIMER EXPIRED AT B WHILE WAITING FOR SRVA FROM F OR G.

Figure 6-21. Timer Expired

K. Incorrect Translation for Primary Destination

10.64 Referring to Figure 6-22, following the final translation at **B**, a Verify form of the SRVT is sent to **X** as identified by the PC resulting from the translation. **X** sends SRVR and SRVA messages indicating success. However, the results of the comparison of the GTT (PPC+SSN) at the mate do not match with the PPC+SSN received in the Compare message at **C**. SRVA 4 message indicates a mismatch. **B** sends SRVR and SRVA messages to **A** indicating an unsuccessful translation. Since the SRVR 6 message indicates success and the SRVR 5 message indicates the error, the user knows that the error is in translation at **C** and not at **B**.

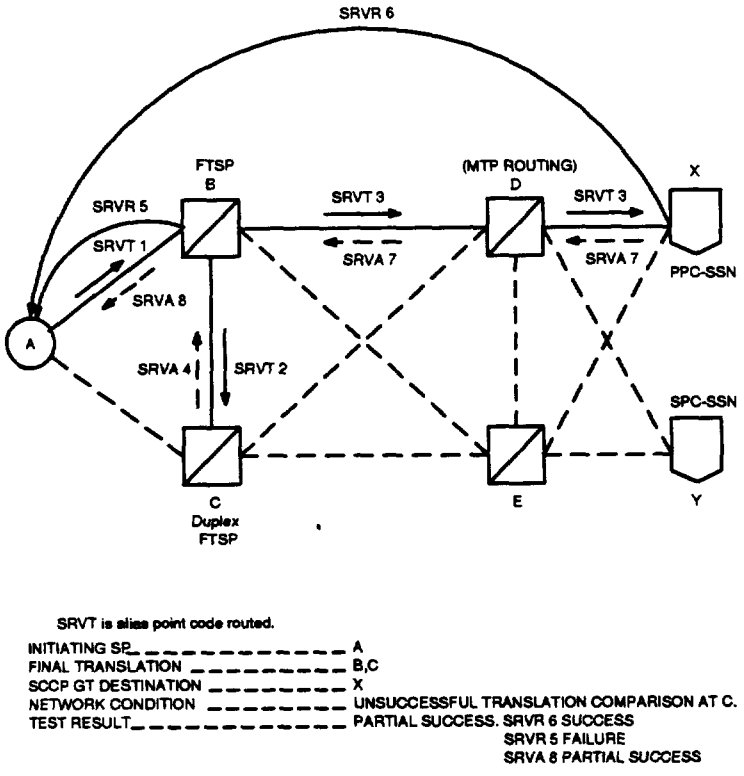


Figure 6-22. Incorrect Primary Translation

L. Incorrect Translation for Secondary Destination

10.65 Following a final GTT at **B** (Figure 6-23), SRVT messages are sent towards the destinations identified by PPC+SSN and SPC+SSN. This occurs before the arrival of the results of the comparison performed at **C**. The comparison at **C** is successful for PPC+SSN but unsuccessful for SPC+SSN, and these results are reported to **B** via SRVA 4 message. The primary destination reports success via SRVR and SRVA messages. Because the translation for the secondary destination is in error, the message is received by **H** (absent the translation error the message was destined for **G**). The destination **H** sends SRVR and SRVA messages. It reports that it does not serve the GT in the message. The error reported is "Not Secondary Destination." From the SRVR and SRVA messages received, the user can identify **B** as the source of the error of the GTT for the secondary destination.

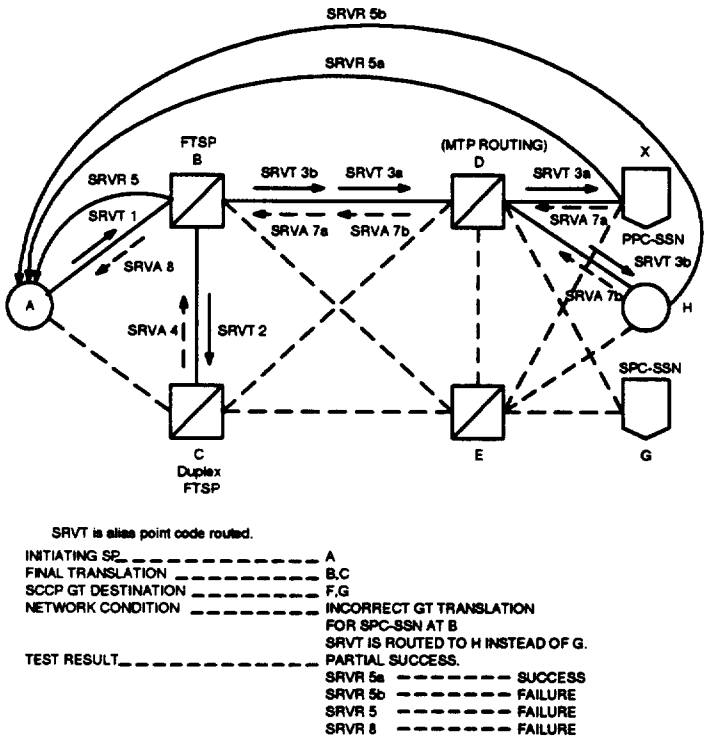


Figure 6-23. Incorrect Secondary Translation

M. Incorrect Translation for the Intermediate TSP

10.66 **B** performs (Figure 6-24) the intermediate translation which identifies (by point code) the next TSP as **D**. **D** performs the final translation and identifies the destination as **X**. **X** reports success via SRVR and SRVA messages. The results of the comparison of the intermediate translation at **B** and that performed at **C** indicate that the comparison is unsuccessful. These results are reported by SRVA 4 message to **B** and conveyed to the Initiating SP by SRVR 5 message and SRVR 12 message. The results indicate translation at **B** is correct. This mismatch is due to the translation error at **C**.

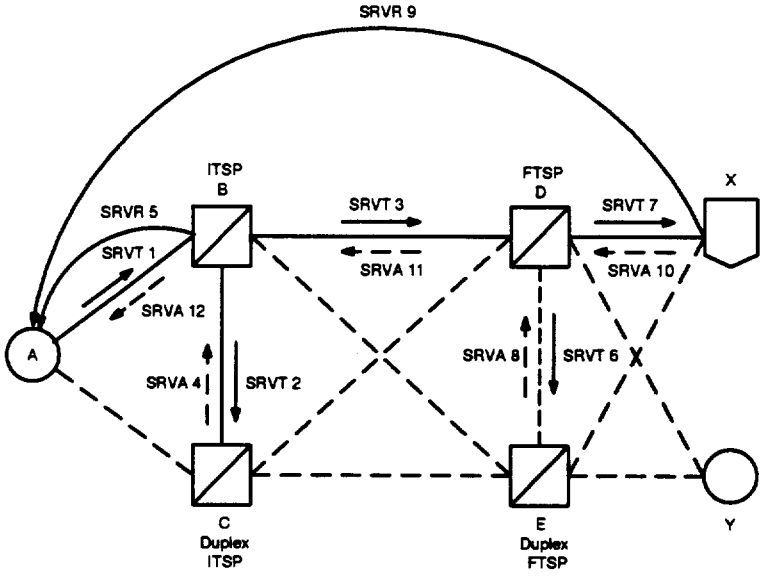


Figure 6-24. Incorrect Translation for the Intermediate TSP

N. Destination Does Not Serve the GT in the SRVT Message

10.67 **B** performs the final GTT and sends forward SRVT 3 to **D** which MTP routes it to **Z**. **Z** examines the GT in the message received and concludes that it does not recognize the GT in the message. Since the SRVA 4 message reports a successful comparison, it implies that the error is in **B** as well as **C**. The error detection scenario in Figure 6-25 is representative of the following errors.

(1) Not Primary Destination

(2) Not Secondary Destination

(3) Primary Destination Not Recognized

(4) Secondary Destination Not Recognized.

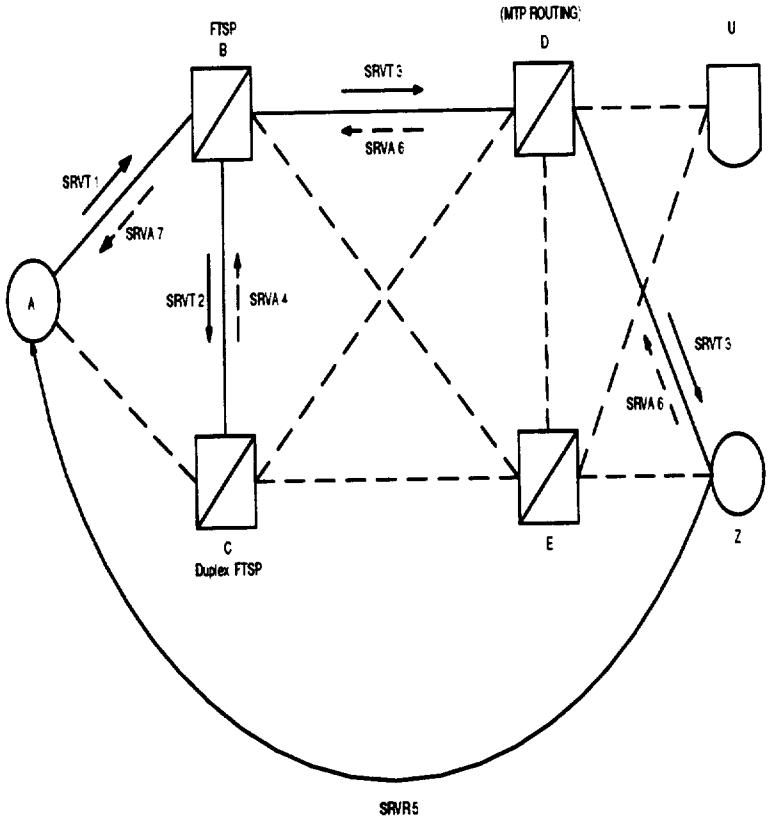


Figure 6-25. Destination Does Not Serve the GT in the SRVT Message

O. Unrecognized Point Code From Translation

10.68 **B** performs the intermediate translation and forwards the SRVT message to **D** (Figure 6-26). **D** performs the final translation; however, **D** does not recognize the point code of **F** resulting from the translation (MTP routing error). **D** sends an SRVR message to the initiator. The error is identified by the SRVR and the SRVA messages.

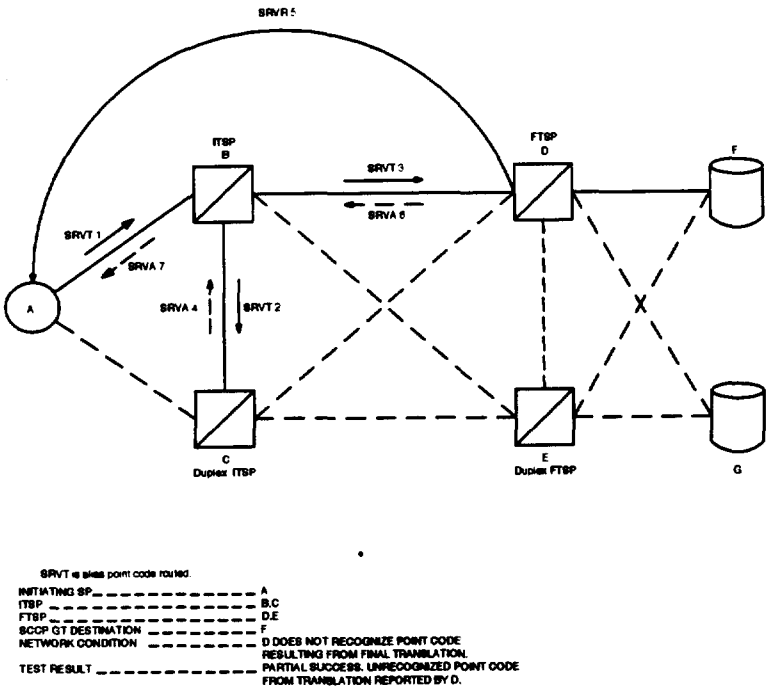


Figure 6-26. Unrecognized Point Code from Translation

P. Wrong SP

10.69 **F** receives a Request form of the SRVT message from **D** which should have performed the final translation (Figure 6-27). **D** has committed the error since the message should have been the Verify form of the SRVT message. The Request form of the SRVT message does not contain the SSN whereas the Verify form does contain the SSN. **F** reports the error via the SRVR and the SRVA messages.

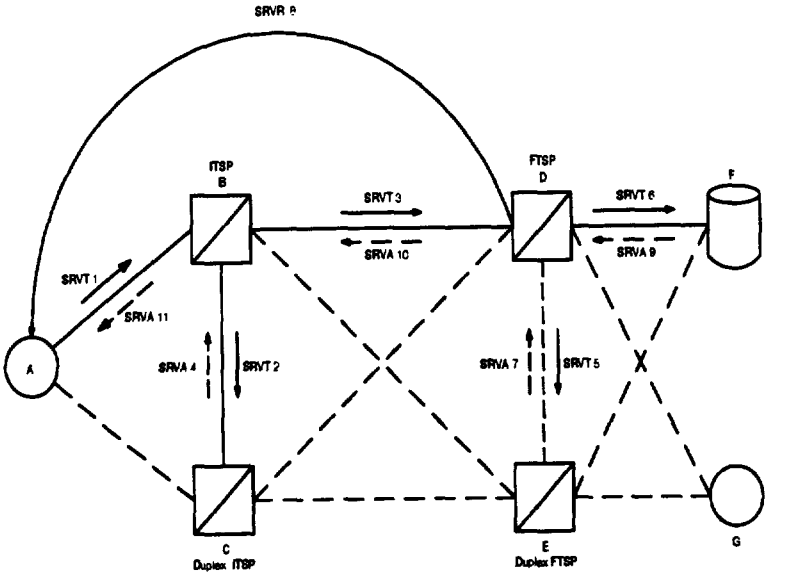


Figure 6-27. Wrong SP

Q. SRVT Bypasses Linkset Failures

10.70 **B** performs the intermediate and **E** the final GTT (Figure 6-28). Because the SCCP route **B-D** is blocked, route **B-E** is selected (**D** and **E** are aliased) and **E** sends forward SRVT messages for destinations **X** and **Y**. The destinations **X** and **Y** report success by SRVR and SRVA messages.

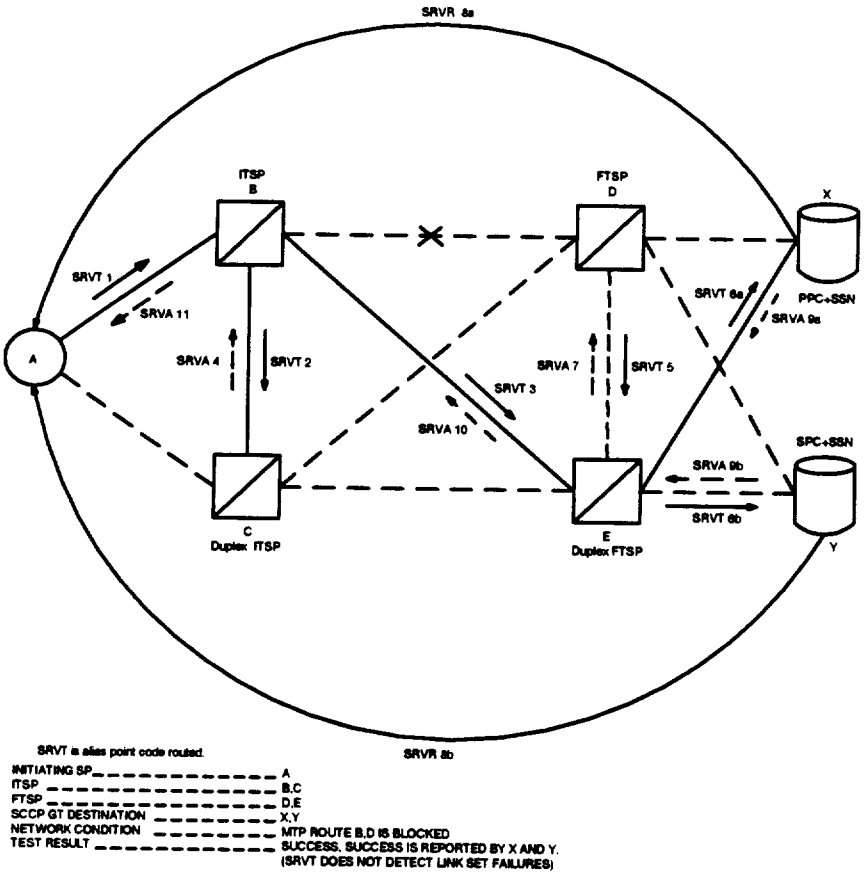


Figure 6-28. SRVT Bypasses Linkset Failure

Reporting of Test Results

10.71 This section clarifies and augments the error detection and reporting process. Each error is identified in the SRVR and SRVA message. The SRVA message has the capability to report more than one error. The SRVR message reports only one error. In the case of failure or partial success, the SRVA message always contains the information regarding whether or not the SRVR message was sent. The SRVR message contains the point code of the SP where the error was detected and may contain a trace of the TSPs. The printout report lists 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 that are listed.

10.72 The declaration of "success" takes place at the tested destination if the procedure is successful and no errors have been detected and no difficulties have been encountered in sending back the SRVR (if requested) and SRVA messages from the destination. Although the tested destination has declared success in the SRVR message to the initiator (not having the FTSP function), the initiator will also get an SRVR and an SRVA message from a duplexed TSP indicating a failure if the results of comparison of the GTT did not match with the translation at the mate. This is because the duplexed TSP forwards the SRVT message to the tested destination prior to receiving and analyzing the results contained in the SRVA message from its mate.

A. Error in SRVT Initiation

10.73 The initiating SP detects this error, which pertains to the validity of the data in the SRVT initiation command.

B. Loop Routing

10.74 An SCCP routing loop is detected when an *A-I-Net* products STP acting as a TSP finds that the point code of the next TSP or that of its mate is already on the list of crossed TSPs in the SRVT message.

C. Excessive Length Route

10.75 An excessive length route is detected by an *A-I-Net* products STP acting as a TSP prior to forwarding the SRVT message to the next TSP or to the destination SP. The error is detected when the *A-I-Net* products STP examines the list of crossed TSPs contained in the SRVT message and finds that the number of crossed TSP(s) has equaled or exceeded the threshold parameter **N** value contained in the message.

10.76 If the results of an SRVT test indicate that the excessive length threshold has been exceeded, the user should reinitiate the test using a higher value of parameter N so as to test for further errors. When other errors (if detected) have been corrected, the user can then address the issue as to whether there is actually a routing error

causing the excessive length threshold to be exceeded, or the number of TSPs is greater than the suggested value.

D. No Translation for Global Title

10.77 This error is detected by an *A-I-Net* products STP acting as a TSP. The TSP may be assigned the intermediate translation or the final translation function for this Global Title. The error implies that there is no point code corresponding to this GT at the ITSP and no PPC+SSN, SPC+SSN (optional) corresponding to this GT at the FTSP.

E. Inaccessible Signaling Point

10.78 This error is referred to as "Route Inaccessibility." It is detected at the initiating SP or at a TSP. It is never reported from the destination SP. Route inaccessibility means that in the course of attempting to forward the SRVT message to the TSP or the tested destination, an SP encounters one or more of the following situations.

(a) **Congestion:**

The SCCP route selected for forwarding the SRVT to the next SP is congested and the message priority does not permit its transmittal.

(b) **Blockage:**

All routes to the intended SP are blocked, for example, as a result of linkset failures, or the destination SP has encountered signaling point isolation.

(c) **Crossing Network Boundaries:**

The SRVT message will not be allowed to be sent to a nonlocal network by the *A-I-Net* products STP. This condition is also treated as a "Route Inaccessibility" error. The switch is not required to detect or stop SRVT messages from going across the network boundary.

(d) **Not SS7 Equipped:**

If the SRVT message cannot be forwarded to an SP because of lack of resources (the interconnecting network to the SP is non-SS7 or a noncompatible version of SS7 protocol), it is to be treated as a "Route Inaccessibility" error for the purposes of reporting via SRVA and SRVR messages.

(e) **Subsystems Prohibited:**

This error is reported if the SRVT message is destined for a prohibited subsystem.

(f) **Receiving Unitdata Service Message:**

This error is reported when a Unitdata Service Message is received in response to an SRVT message sent.

If the error is detected at the initiating SP, the cause of inaccessibility is uniquely identified with a suffix letter in the error code.

Test Cannot Be Run Due to Local Conditions

10.79 The inability to initiate the test at the initiating SP (or the initiating SP with TSP functionality) or the inability for the test to be continued at a TSP as a result of local conditions results in this error condition. Local conditions prohibiting the initiation at an SP are:

(1) Processor overload.

(2) The test pertains to a GT which is already under test.

(3) The threshold for maximum number of initiations at an initiating SP has already been reached.

10.80 The error code uniquely identifies each error condition at the initiating SP. Local conditions prohibiting the continuation of an SRVT at a TSP are:

(1) Processor overload.

(2) The threshold for the maximum number of SRVT tests running at a TSP has already been reached.

10.81 If the test is initiated at an *A-I-Net* products STP acting as a TSP, then the prohibitions at the initiator as well as those at the TSP both apply.

A. Unknown Initiating Signaling Points

10.82 This error is detected at the tested destination or at an *A-I-Net* products STP acting as a TSP. If the SP which is required to send an SRVR message determines that the MTP Backward Routing Indicator was not set or if the MTP Backward Routing Required Indicator was set but the initiator's point code is not recognized in the SRVT message received, then an SRVR message cannot be sent. The error "Unknown Initiating Signaling Point" is identified in the SRVA message sent by the SP.

10.83 In the above discussion, if there is a TSP en route from the error detecting SP to the initiating SP, the TSP will attempt to send an SRVR message and report the unknown initiator it received in the SRVA message. It will also send an SRVA message. If the TSP determines that the MTP Backward Routing Required Indicator was not set or that the MTP Backward Routing Required Indicator was set but the Initiator's PC is not recognized, it cannot send the SRVR message. It sends an SRVA message indicating an SRVR message was not sent and that the initiator is unknown.

B. Timer Expired

10.84 The error condition "Timer Expired," also referred to as "Time-Out Waiting for SRVA(s)," is detected at the initiating SP or at a TSP. It does not apply to the tested destination. The SRVR message also contains the point code(s) of the SP which did not send the SRVA message(s).

C. Message Arrived at the Wrong Signaling Point

10.85 If any signaling point which is not a duplexed TSP receives a Compare form of the SRVT message or a duplexed TSP receives a Compare form of the SRVT message from a TSP which is not its mate, it reports this error to the initiating SP. If a Request form of the SRVT message arrives at an SP which is not a TSP, it also reports this error. If a Verify form of the message is received at a TSP or at any SP which is not the tested destination, it also reports this error.

D. Incorrect Translation for Primary Destination

10.86 This error is detected by the mate of a duplexed FTSP and indicates that the translation result pertaining to PPC+SSN at the mate does not match with the results at this FTSP. The error is identified in the SRVA message. The SRVR message also identifies the mate performing the comparison and identifies the error.

E. Incorrect Translation for Secondary Destination

10.87 This error is detected at the mate of a duplexed FTSP. It is similar in all respects to the discussion for "Incorrect Translation for Primary Destination" except that the mismatch concerns PPC+SSN rather than PPC+SSN.

F. Incorrect Translation for the Intermediate TSP

10.88 The error is detected by the mate of a duplexed FTSP and indicates that the translation result pertaining to PPC or SPC or both does not match with the results at the ITSP. The SRVR message also identifies the mate performing the comparison and identifies the error.

G. Not Primary Destination

10.89 The error is detected at the primary of a mated pair of SCPs when the SCP determines that it does not serve the GT as the primary destination. The error is also reported by a nonmated SCP or a switch when it determines that it does not serve the GT contained in the SRVT message.

H. Not Secondary Destination

10.90 The error is detected at the secondary of a pair of mated SCPs when the SCP determines that it does not serve as a secondary for the Global Title contained in the SRVT message. The error is also detected at a switch or nonmated SCP which is addressed as secondary for the GT contained in the SRVT message.

I. Primary Destination Not Recognized

10.91 The error is detected at the secondary of a pair of mated SCPs when the SCP determines that it does not recognize the PPC+SSN as the primary destination for the GT contained in the message. (It does recognize the SPC+SSN as the secondary destination of the GT which it serves.)

J. Secondary Destination Not Recognized

10.92 The error is detected at the primary of a mated pair of SCPs when it determines that it does not recognize the SPC+SSN in the SRVT message as the secondary destination for the GT contained in the SRVT message. (It recognizes the PPC+SSN as the primary destination which it serves.) The error is also detected at the switch or a nonmated SCP which receives an SRVT message indicating that the recipient is the primary destination but a secondary destination is also included in the message.

Unrecognized Point Code from Translation

10.93 This error is detected at a TSP or initiating SP when it cannot route on the point code realized from the Global Title translation. The point code may pertain to another TSP or that of the destination SP.

Test and Acknowledgement Messages for the SRVT

10.94 The SRVT uses three OMAP messages. All the SPs must be able to send and receive these messages:

(a) The SCCP Route Verification Test (SRVT) Message

(b) The SCCP Route Verification Acknowledgement (SRVA) Message

(c) The SCCP Route Verification Result (SRVR) Message.

A. SCCP Route Verification Test Message

10.95 The SRVT Message will have three forms:

- The SRVT Request Message
- The SRVT Verify Message
- The SRVT Compare Message.

10.96 The coding of both the Request and Verify forms of the messages will be identified by "No Compare" setting of the form indicator in the message.

10.97 The SRVT Request message is sent by the SP which is initiating the SRVT procedure. All signaling points in the network have the capability to send and respond to this message.

10.98 The Verify form of the message is sent from an FTSP to the tested destination.

10.99 The *A-I-Net* products STP has the capability to send the Compare form of the SRVT message.

B. SCCP Route Verification Acknowledgement Message

10.100 The SCCP Route Verification Acknowledgement (SRVA) message will be sent in response to the SRVT message and will contain the results of the test. The message is sent back using the OPC contained in the SRVT message.

10.101 In the case of failure or partial success, the SRVA message will identify whether an SRVR has been sent. The SRVA message will identify the success of the test, or in case of a failure, the cause of the failure.

C. SCCP Route Verification Result Message

10.102 The SCCP Route Verification Result (SRVR) message will be sent from an SP which stops the test to the SP which initiated the test and will contain the test results, whether success or failure. In the case of failure or partial failure, it will identify the cause and contain the point code(s) information.

10.103 The message is sent back to the initiator (if requested in the SRVT Message to which it is responding) using the initiator's point code contained in the SRVT message if the MTP Backward Routing Indicator was set.

Input Messages for the SRVT

10.104 For the input message associated with this feature, refer to the appropriate system I/O manual for the correct format.

10.105 The initiation command can be issued locally at the initiator SP or remotely via one or more OSs. The test results will be reported to the system initiating the test. Syntax errors will be reported using standard PDS/MML error handling.

A. SRVT Initiation Command

10.106 The SRVT initiation command is:

EXC:SRVT;TYPE a[. . . .etc].

B. Supplemental Command

10.107 The supplemental command is not a part of the SRVT procedure. The user may use the command prior to initiating the SRVT to determine if the SP associates

more than one TPC with a given Translation Type (TT). The user could then specify one of the TPCs in the SRVT initiation command, in which case the SP would address an SRVT Request message only to that TPC.

10.108 An SP that is required to respond to an SRVT initiation command is also required to respond to a supplemental command and deliver the response to that source. This command is used to determine where the SP would direct an SCCP message with a given TT for GTT.

10.109 By sending such a message to a translation signaling point for GTT, the SP would respond with a list of all TPCs to which the SP could address the message. These TPCs could be true or Alias point codes. If the SP would perform the GTT for the given TT, the SP would respond with its own true point code. If the SP would neither perform the GTT itself nor send the message elsewhere, the response would be "UNABLE TO DERIVE TPC." **Format**

10.110 The supplemental command is:

OP: TPC; TYPE a

The parameter a denotes a specific TT or "ALL."

C. SRVT Delay Parameter Command

10.111 The purpose of this command is to change or display the Delay parameter, which is used on the calculation of the T2 timer. The expiration of the T2 timer signifies the end of the waiting period for the reception and processing of all expected SRVA messages. This command is entered manually or either locally or remotely through an OS.

10.112 If the initiator is not a TSP, it should set:

T2 = D(SRVT) * (N(SRVT)+1)

where N(SRVT) is the maximum number of TSPs crossed, and D(SRVT) is an administered value.

10.113 If the initiator is a TSP for the GTI + GT, then it should set the timer based on the equation:

T2 = D(SRVT) * N(SRVT)

to take into account the fact that only TSPs are added to the list of points crossed and counted towards the threshold.

10.114 An intermediate or final TSP should set the timer based on the equation:

T2 = D(SRVT) * (N(SRVT) - Number of Transactions Completed

Note that T2 at a TSP will always be a positive number because if the number of translations in the trace was greater than or equal to N(SRVT), an excessive length route would have been detected and the test would be discontinued prior to the setting of T2.

Format

10.115 The command for the Delay parameter is:

CHG:SRVT[a]!

The parameter (**a**) is the new value of the Delay parameter, and has a valid range of 8 - 16 seconds, inclusive. The initial default is 12.

Output Messages (Reports) for the SRVT

10.116 For the SRVT output formatted results, refer to the appropriate system I/O manual.

A. Test Restrictions

10.117 To alleviate concerns for demands on processing resources, the number of simultaneous SRVTs at the initiating SP is restricted to 5.

B. Translation Signaling Point

10.118 An *A-I-Net* products STP acting as a TSP will be allowed to process no more than 25 concurrent SRVT tests. This includes five tests allowed as an initiating SP.

C. Destination SP

10.119 There is no limit on the number of concurrent SRVT tests allowed to terminate at a destination SP. The number of tests allowed for simultaneous initiation is, however limited to five as stated earlier.

D. Relation Between SRVT and MRVT

10.120 The SRVT provides SCCP level routing verification that includes the MTP level routing verification capability. The MTP level routing of the SRVT test messages to the translated TPC is required to determine the accuracy of the performed GTT. Because SRVT does not sectionalize problems in MTP routing, the MRVT is a prerequisite for the SRVT.

10.121 Specific similarities and differences between MRVT and SRVT are highlighted in the MRVT versus SRVT comparison presented in Table 6-N.

Table 6-N. Comparative Analysis of SRVT Versus MRVT

Basis of Comparison	MRVT	SRVT	Remarks
Purpose	Test procedure for MTP Routing Verification in SS7 Network.	Test procedure for SCCP level route verification in SS7 Network. Provides means for testing the GTT service of the Signaling Connection Control Part (SCCP).	An indication of failure or inconsistency is reflected in the messages received at the initiating SP.
Test Messages	Uses three OMAP Messages: MTP Routing Verification Test Message (MRVT) MTP Routing Verification Acknowledgement Message (MRVA) MTP Routing Verification Result Message (MRVR).	Uses three OMAP Test Messages: SCCP Routing Verification Test Message (SRVT). SCCP Routing Verification Acknowledgement Message (SRVA). SCCP Routing Verification Result Message (SRVR). In addition, the SRVT message in "Compare" form is used by STP to Compare GTT results with the data in the mate STP.	Test approach for MRVT and SRVT is similar. Test messages perform identical roles except for Compare form of SRVT which is used to compare results of mated translation points. Also, SRVT carries much more information than MRVT message (identification of primary and addition of the secondary Destination Point Codes and Subsystem numbers).
Functionality	Verifies all MTP level routes between any two signaling points in the network. Checks for routing loops. Checks for excessive length routes. Checks for routing accuracy in both directions. Tests unknown destinations. MRVR sent to originating SP on normal call if no routing entry at a Signaling Transfer Point (STP).	Verifies GTT data for accuracy, completeness, and consistency. Verifies SCCP level routing and depends on MRVT for verification of MTP level routes. Checks for loops in SCCP routes. Checks for routing accuracy in both directions on SCCP routes. Tests for unknown destinations.	The SRVA and SRVR identify many other causes of failure that MRVA and MRVR do not. There can also be multiple physical destinations for SRVT.

Table 6-N. Comparative Analysis of SRVT Versus MRVT (Contd)

Basis of Comparison	MRVT	SRVT	Remarks
Standard Perspective	Lucent Technologies implementation meets CCITT and ANSI OMAP standard.	Lucent Technologies implementation meets CCITT and ANSI OMAP standard.	
Intranet Operation	Will check routes up to and including gateway signaling points.	Will check GTT data for accuracy at translation point.	
NI	Network Interconnect Operation already specified in the protocol. Will require TCAP interoperation capability between network not using the same version of TCAP.	The SRVT protocol needs to be enhanced for Network Interconnect Operation. Will also require TCAP interoperation capability between network not using the same version of TCAP.	Screening of OMAP messages at Gateway STPs is applicable to MRVT as well as SRVT. The route trace information for MRVT does not cross network boundaries. The NI Operation for SRVT remains to be defined via the standards process.
Network Elements Impacted	1A ESS™, 4ESS™, 5ESS® Switch (Initiating SP, Destination SP) STP (Initiating SP Transit SP, Destination SP) NCP (Initiating SP or Destination SP) SCP (Initiating SP or Destination SP)	1A ESS (Initiating, Destination) 4ESS (Initiating, Initiating/ Final Translation, Destination) 5ESS (Initiating, Destination) STP (Initiating, Translation) SCP (Initiating, Destination)	
Uses	Verify installation of recent changes to MTP routing data. Troubleshoot routing problem. Repair verification.	Verify installation of recent changes to translation data (SCCP data). Troubleshoot translation data and SCCP routing problem. Repair verification.	Repair verification implies verification following correction of error or fault.

Table 6-N. Comparative Analysis of SRVT Versus MRVT (Contd)

Basis of Comparison	MRVT	SRVT	Remarks
Limitations and Constraints	Verifies master copy of administered data. Other tools are required to verify copies of administered data and dynamic data.	Verifies master copy of administered data. Other tools are required to verify copies of administered data and dynamic data. The SRVT does not check all MTP level routes to destination.	The MRVT is necessary along with SRVT if accuracy of GT data as well as all MTP routes need to be tested.

11. Message Trap

11.01 The message trap feature is intended to assist in the isolation of problems in an SS7 network. The message trap collects and prints signaling messages used in an SS7 network as they are passed through SS7 link nodes on the CNI ring. It does this without hampering normal processing of signaling messages.

11.02 The message trap is not intended to be a complete protocol analyzer with extensive processing capability. Rather, it is intended to be used on selected situations with a small set of possibilities. The trap can be tailored to a specific set of information within the message effectively narrowing the amount of output.

11.03 For a quick reference of the message trap capabilities, refer to 256-090-136, *Message Trap Job Aid.*

Overview of Trap Operation

11.04 A trap can be initiated by a technician at a switch, STP, or remote support system. However, since the trap only matches on incoming or outgoing messages (this choice is generic dependent), two signaling points may be required to trap a call sequence. Time relationships between different messages for a particular call cannot be determined using message trap; some other means is needed.

11.05 When a trap in a link node has been entered and activated, all messages coming in to or going out of the node are matched against the attributes of that trap. Some or all of the matching signaling messages are collected in a buffer. Periodically, this buffer is sent to the 3B20D computer where the signaling messages are collected and may be written to a disk file for later output and/or displayed in real time. Results in a disk file are saved until they are overwritten with new messages or are purged by the technician. The technician may send the trap output to the MCRT, ROP, or a support system. The message trapping rate determines how many of the messages matched by the node are actually trapped and saved for output.

11.06 The trapping and message translation processes are continuously monitored by the system to ensure proper operation. When a trap is started, the 3B20D computer notifies the link node of the new trap and expects the node to acknowledge the trap. If an acknowledgment is not received, an error is indicated. Furthermore, even after acknowledging the trap, the health of the node is continuously monitored and reported to determine whether or not it changes state.

11.07 A change in a node's state, such as going Out-Of-Service (OOS), can cause the node to abort a trap. Traps are also aborted due to exhaustion of computer resources or congestion in the ring or 3B20D computer. Also, initialization of the 3B20D computer results in termination of all active traps (and any trap data stored in main memory is lost). Trapped message data on disk is not lost due to termination of traps.

Input Message Summary

11.08 Various input commands are used to manipulate traps. Refer to the application input or output message manuals for specific details. For the *A-I-Net* products STP version, MCRT pages 1116,1117 support these messages with pokes that generate the same syntax as typed in directly.

11.09 The primary commands are:

- **SET:TRAP** to initiate traps and set trap parameters
- **OP:TRAP** to display trap results or display trap status
- **INH:TRAP** to temporarily stop a particular trap
- **ALW:TRAP** to allow an inhibited or future trap operation
- **STOP:TRAP** to terminate and initialize trap resources when necessary.

The SET:TRAP Command

11.10 The **SET:TRAP** command allows the technician to enter all the parameters of the trap and possibly activate the trap. The system identifies each trap with a trap identification number. This number is then used with the **OP:TRAP** command to output trap results.

11.11 The **SET:TRAP** message can be built in three parts, the first of which is mandatory and the other parts are optional in that certain defaults are invoked if not entered. The clauses are separated by the appropriate punctuation (; or :) depending on the type of input message syntax used. The three parts of the trap message can be described as (1) where (which nodes) to trap data on, and what message types to trap on, and which mode; (2) what specific message data to trap on; and (3) how to administer the trap.

A. Specifying Which Links to Trap On

11.12 The trapping of messages on a link or set of links can be specified such that each signaling element can be tailored to the situation. The use of the **LNKSET**, **LNKLST**, and **LNKR** keywords will be determined by the amount of links to be covered by the trap in context of the situation to be handled. When making the choice, remember that the messages are going to be distributed over all the links in a linkset as well as possibly over more than one linkset. This field must be specified.

B. Specifying Which Message Type to Trap

11.13 The process of choosing which types of messages can be as simple as defaulting to all SS7 messages (**MTYPE ALL7**). The message type options are:

- Signaling Network Management (**SNM7**)
- Integrated Services Digital Network (**ISDN7**)
- Signal Connection Control Part (**SCCP**)
- Network Test and Maintenance Regular (**MREG7**)
- Network Test and Maintenance Special (**MSPEC7**).

Note that the Input/Output manuals will show other message types that are not used for SS7 Signaling.

C. Specifying the MODE

11.14 The **MODE** parameter is available with 1AP3D, 5E7, 4AP9, *A-I-Net* products STP Release 0 and *A-I-Net* products SCP Release 1 software releases. The use of this parameter will control if incoming OR outgoing messages will be trapped. IT IS NOT POSSIBLE to trap both directions simultaneously on the same node. The default is incoming traps if not specified.

D. Specifying Specific Message Data to Trap On

11.15 Signaling messages are trapped based on the value of certain fields in the message. The technician can specify values for up to five parameters from the predefined list of parameters for the basic message types. Table 6-O shows the association of the different SS7 message types and the associated predefined parameters contained within those types of messages. Optional masks (**MS** parameter) can also be specified for these parameters to aid in trapping a particular situation.

NOTE:
The defaults for the **MS** parameter are all **x'FF** per byte of data on 5ESS Switches and **x'00** on all other elements. Therefore, specify a mask when using a parameter that has a mask that defaults to **0**. Also, specify an **MS** value when other than the default value of **FF** is needed.

One parameter, the offset byte (**OFSTB**), is not an official parameter of a message, but is instead a parameter that can be used to specify a specific byte(s) anywhere within a particular message. An optional mask (**MS** parameter) can also be specified for this parameter to aid in trapping a particular situation.

Table 6-O. MTYPE and Message Parameter Association

SET:TRAP Parameter Keyword	MTYPE Keyword Value (Notes)						Parameter Description
	ALL7	SCCP	SNM7	MSPEC7	MREG7	ISDN7	
OPC	X	X	X	X	X	X	Originating PC
DPC	X	X	X	X	X	X	Destination PC
CGPC	X	X					Calling party PC
CGSN	X	X					Calling party SSN
CGT	X	X					Calling party GT type
CGGT	X	X					Calling party GT
CDPC	X	X					Called party PC
CDSN	X	X					Called party SSN
CDT	X	X					Called party GT type
CDGT	X	X					Called party GT
RFR	X	X					Reason for return*
OFSTB	X	X	X	X	X	X	Offset to byte
MS	X	X	X	X	X	X	Mask for parameter†

Notes 1:

"X" indicates the parameter is allowed for that message type.

The **MTYPE** keyword is associated with the SERVICE INFORMATION (SI) field in the SERVICE INFORMATION OCTET. The following maps the keyword to the SI value:

ALL7 - All values
SNM7 - 0
MREG7 - 1
MSPEC7 - 2
SCCP - 3
ISDN7 - 5

* Reason for Return (RFR) does not allow an **MS** parameter with it.

† The **MS** parameter must be specified together with another parameter to be effective.

11.16 In order for the **OFSTB** parameter to be used, one must understand the exact layout of an SS7 message. Figure 6-29 shows the general layout of any message in terms of the contents of specific bytes as well as the general formats of each of the types of parameters. Note that there are fixed parameters (**A,B** in the figure) which are fixed in position and fixed in length; mandatory variable length parameters (**C,D**) which are fixed in position but variable in length; and optional parameters. Optional parameters require both a name and a length byte. The pointers are counts of the number of bytes from the pointer byte to the beginning of the parameter. If no optional parameters are in the message, the pointer is all zeros. The end of optional parameters is also all zeros after the last parameter.

11.17 Figure 6-30 shows the layout of a typical IAM. The IAM contains all three different types of parameters; fixed, variable length, and optional. This layout illustrates the variations caused by the variable length parameters. Note that the order of the optional parameters may vary from switch to switch even if they have the same parameters. The protocol does not require a fixed order. See the end of this chapter for examples.

11.18 For specific contents of any message, one must also have access to the appropriate technical references (BELLCORE, ANSI, CCITT, etc.) which spell out the exact contents.

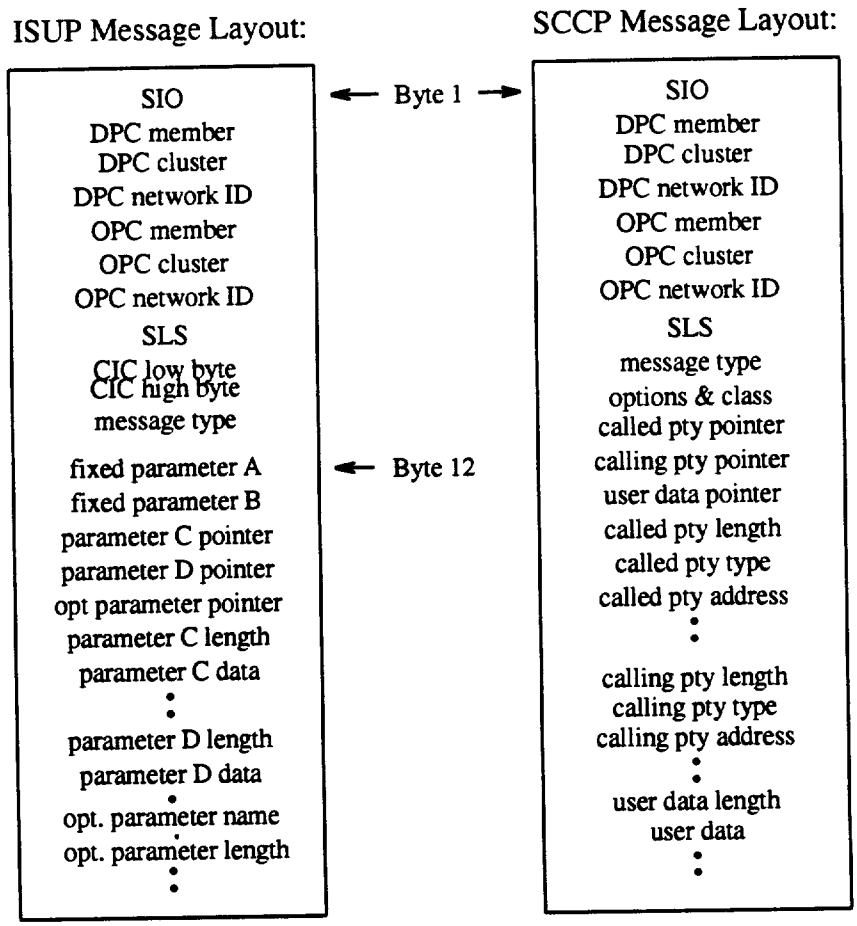


Figure 6-29. SS7 Message Templates

IAM Byte Format for 64 kb, 56 kb, and 3.1 kb (Voice or Modem)				
64 kb Byte#	56 kb Byte#	3.1 kb Byte#	Function Description	
1	1	1	Service Information Octet (95)	
2	2	2	Destination Point Code Member (02)	
3	3	3	Destination Point Code Cluster (1E)	
4	4	4	Destination Point Code Network ID (FA)	
5	5	5	Origination Point Code Member (1C)	
6	6	6	Origination Point Code Cluster (1E)	
7	7	7	Origination Point Code Network ID (FA)	
8	8	8	Signaling Link Selection (1A)	
9	9	9	Circuit Identification Code (2B)	
10	10	10	Circuit Identification Code (OC)	
11	11	11	Message Type (01)	
12	12	12	Nature of Connection (00) *	
13	13	13	Forward Call Indicators 1 (22) *	
14	14	14	Forward Call Indicators 2 (00) *	
15	15	15	Calling Party Category (0A) *	
16	16	16	Pointer to USI Indicator (03)	
17	17	17	Pointer to Called Party Parameters (05) (07) (06)	
18	18	18	Pointer to Optional parameter (0C) (0E) (0D) †	
19	19	19	Length of USI Parameter (02) (04) (03) †	
20	20	20	Data for USI Parameter (88) (88) (80/90‡)†	
21	21	21	Data for USI Parameter (90) (90) (90) †	
	22	22	Data for USI Parameter (21) (A2) †	
	23		Data for USI Parameter (8F) †	
22	24	23	Length of Called Party Parameter (07) †	
23	25	24	O/E and Nature of Address (03) †	
24	26	25	Numbering Plan (10) †	
25	27	26	0	8 †
26	28	27	5	0 †
27	29	28	6	9 †
28	30	29	2	1 †
29	31	30	4	3 †

Note:
Information shown in ( ) indicates the data in these particular bytes for an output message. The values shown for USI are for voice calls. Data Calls will usually be two bytes for 64-kb clear or restricted and 4 bytes for 56 kb rate adapted. The pointers are set up per this example which has a 10 digit called party.

* Fixed Parameters

† Variable Length Parameters

‡ 80 for 3.1 kb voice and 90 for 3.1 kb modem (data)

Figure 6-30. IAM Message Format (Sheet 1 of 2)

IAM Byte Format for 64 kb, 56 kb, and 3.1 kb (Voice or Modem)			
64 kb Byte#	56 kb Byte#	3.1 kb Byte#	Function Description
30	32	31	Name of Optional Parameter-Charge Number (EB) §
31	33	32	Length of Optional Parameter (07) §
32	34	33	Data of Optional Parameter (03) §
33	35	34	Data of Optional Parameter (10) §
34	36	35	Data of Optional Parameter (07) §
35	37	36	Data of Optional Parameter (98) §
36	38	37	Data of Optional Parameter (96) §
37	39	38	Data of Optional Parameter (06) §
38	40	39	Data of Optional Parameter (07) §
39	41	40	Name of Optional Parameter-OLI (EA) §
40	42	41	Length of Optional Parameter (01) §
41	43	42	Data of Optional Parameter (00) §
42	44	43	Name of Optional Parameter-Transit Network-Selection (23) §
43	45	44	Length of Optional Parameter (03) §
44	46	45	Data of Optional Parameter (21) §
45	47	46	Data of Optional Parameter (82) §
46	48	47	Data of Optional Parameter (88) §
47	49	48	Any More Parameters or End of Optional Parameters (00) §

§ Optional Parameters.

Figure 6-30. IAM Message Format (Sheet 2 of 2)

11.19 A trap will fire when the bytes of the message from the input parameters are ANDed with the **MS** parameter. If the result matches the entered data for the given parameter, the trap is triggered and the results sent to the 3B20D computer processor for output to the appropriate device. Any parameters not specified are essentially "don't care." This allows messages to be trapped in either broad or specific terms. Note that using multiple parameters is an ANDing of all the conditions such that all must be true for the trap to fire.

E. Administering the Trap

11.20 Any of the following parameters can also be specified. These parameters are not used to match fields in the signaling message.

(a) **ST**—The network time to start trapping messages.

(b) **DUR**—The maximum duration of the trap.

(c) **MCNT**—The maximum number of messages to be trapped.

(d) **MGSZE**—The number of bytes to save from each trapped message.

(e) **RATE**—The rate of trapping, specified as one out of every "x" messages matching the trap criteria.

(f) **DEST**—The destination to which the **SET:TRAP** response should be sent.

(g) **RTDSP**—Whether or not to output trap results in real time; that is, as soon as they are collected by the central processor. If this is specified as "**N**", the user must enter the **OP:TRAP** command to output the results.

(h) **SAVE** - Whether or not to save trapped message data on disk. Unless real time display is "Y", message data must be saved to disk.

The defaults for the preceding parameters are shown in Table 6-P.

Table 6-P. Defaults for Trap Parameters

Keyword	Definition	Default	Range or Format
ST	Start Time	Immediately	Time in 24-hour format
DUR	Duration	(See Table 6-P	168 hours maximum
MCNT	Message Count	(See Table 6-P)	Up to 1000
MGSZE	Message Size	5E = 272 bytes All others=40	Multiples of 4 bytes
RATE	Trap Rate	1/100	Maximum of 1/1;1/N
DEST	Output Destination	MCRT,ROP,SCCS	Any valid output class
RTDSP	Real Time Display	N	Y or N
SAVE	Save on Disk	SAVE	SAVE or NOSAVE

Table 6-P. Defaults for Trap Parameters (Contd)

Specified		Value Used		
DUR	MCNT	DUR	MCNT	ELEMENT
N	N	5MIN	10	5ESS Switch®, 4ESS™ Switch,*A-I-Net* STP ®
N	N	15MIN	10	1A ESS
Y	N	DUR	100	ALL
N	Y	168HR	MCNT	ALL

F. Example of the SET:TRAP Command

11.21 A typical example of the **SET:TRAP** command is shown in Figure 6-31.

5ESS Switch and *A-I-Net* STP

```
SET:TRAP,LNKSET=3,MTYPE=ISDN7:OPC=H'DCC177,OFSTB=10&H'0900,
MS=H'FF00: MCNT=100,RATE=1,RTDSP=Y;
```

1A ESS and 4ESS Switches

```
SET:TRAP,LNKSET 3,MTYPE ISDN7;OPC X'DCC177,OFSTB (10,X'0900),
MS X'FF00; MCNT 100,RATE 1,RTDSP Y!
```

the response is:

```
REPT MON_TRAP
MTRP: TRAP STARTED:ID=4

SET TRAP
MTRP: SET TRAP COMPL; ID ASSIGNED; ID = 4
```

Figure 6-31. Typical SET:TRAP Command

11.22 The situation illustrated is to trap all answer messages from a particular point code. The ANSWER message is an ISDN7 type and the combined linkset is used so that it does not matter which link it arrives on. The **LNKSET** and **MTYPE** parameters set up the links and message type; this part of the command is mandatory. If all links are desired on a switch, it is easiest to simply use the combined linkset number.

11.23 The **OPC**, **OFSTB**, and **MS** parameters constitute, in this example, the part that tailors the trap for a particular situation. There can be at most five parameters in this part.

11.24 In the example, the **OFSTB** offset is shown as 10 since we are interested in the eleventh byte. This is the byte number of the message field to be matched; starting with the Service Information Octet (SIO) byte as "1." The **OFSTB** value (shown as 0900) matches its low byte with an even byte in the message and matches its high byte with an odd byte in the message. Thus, this example matches an odd byte. If an even byte was to be matched, the value would have been 0009. Note that the order of the bytes is shown in a right to left order. This is important to be remembered.

11.25 The **MCNT**, **RATE**, and **RTDSP** parameters constitute, in this example, the part that controls trap administration.

The OP:TRAP Command

11.26 This command allows the technician to obtain status information and/or trap results for any trap, active or otherwise. The time required to retrieve and print trapped messages is normally minimal (it is largely dependent on the number of trapped messages).

11.27 The **OP:TRAP** command provides either general status for all traps or outputs status and data for a specific trap. In the latter form, if signaling messages are trapped, data for each trapped message is output using both a hexadecimal dump of the message and a list of key fields printed in a readable format.

11.28 Figure 6-32 is a typical **OP:TRAP** command output message.

Specifying the Parameters to Control Output of Trap Data

11.29 The parameters to the command are:

(a) **Trap Identification Number**—This is the number created by the **SET:TRAP** command. If not specified, the status of the 32 most recent traps set within the last 24 hours is displayed.

(b) **Real time Display**—Works the same as in **SET:TRAP**.

(c) **Output Class**—Works the same as in **SET:TRAP**.

(d) **Long Form**—Whether or not the long form of trap status display is to be used.

11.30 To obtain trap data output, use the OP:TRAP command as shown in Figure 6-32.

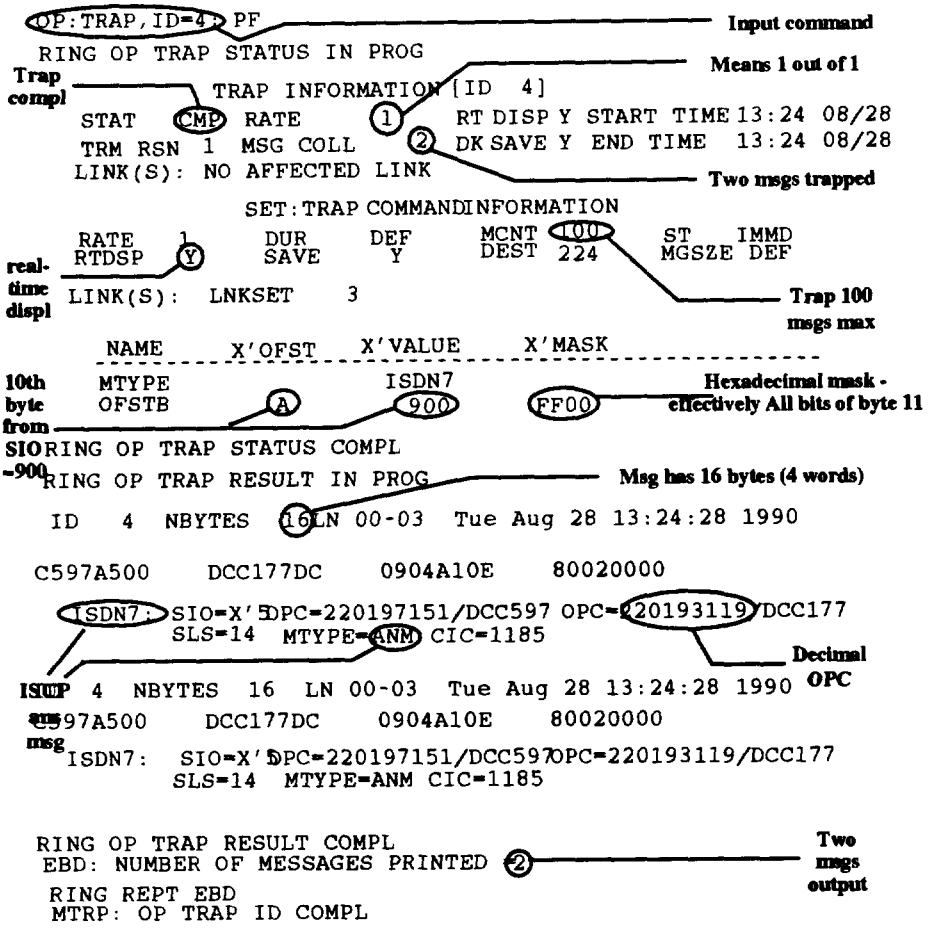


Figure 6-32. Typical OP:TRAP Output Message

A. Examples of the OP:TRAP Command

11.31 To obtain the status of all traps, enter the following command:

`OP:TRAP;` (for 5ESS Switch, *A-I-Net* STP, and *A-I-Net* SCP)

`OP:TRAP!` (for 1A ESS Switch and 4ESS Switches)

11.32 A typical response is shown in Figure 6-33.

```
RING OP TRAP STATUS IN PROG

TRAP      TRM                                          RT    DK   MSG
 ID  STAT RSN RATE    START TIME      END TIME        DISP  SAVE COLL
  4   CMP  1      1  13:24  08/28   13:24  08/28       Y     Y   104
  5   TRM  3      1  13:26  08/28   13:26  08/28       N     Y     0

RING OP TRAP STATUS COMPL

RING REPT EBD
MTRP: OP TRAP COMPL
```

Figure 6-33. Example of OP:TRAP Command Output

B. Analyzing Message Trap Raw Output Data

11.33 Some message data of interest is only displayed as raw data in the message trap output. The user must determine which byte in that raw data corresponds to the message data of interest and convert the byte from hexadecimal to a useful value. Figure 6-30 together with the appropriate reference document must be used as a guide to locating important signaling message fields in the message trap raw output data. Figure 6-30 shows the byte numbers for ISUP and SCCP message data fields.

11.34 Figure 6-34 shows the layout of the typical output message. Notice that certain fields are interpreted for you. The first byte (rightmost) in the first word is always a zero. Also note the order of the bytes within a word and the order of the words. If more than one line of data is output, the words in each line are read left to right with the individual bytes read right to left within a word.

Data from ISUP Trap Output Message:

```
ID 4   NBYTES 16   LN 00-03  Tue Aug 28 13:24:28 1990

DPC     SIO    OPC     DPC     Msg Type   CIC   SLS   End of Data   Byte #

C107A500        DCC177DC        0904AI1E        80020000
 3 2 1           7 6 5 4         11 10 9 8          12

ISDN7: SIO=X'5   DPC=220193007/DCC107   OPC=220193119/DCC177
       SLS=14    MTYPE=ANM  CIC=1185
```

Figure 6-34. Correlation of OP:TRAP Raw Data to Signaling Message Fields

Note the following when analyzing message trap data:

(a) How often does a particular error/fault occur?

(b) Is there a pattern to the errors/faults, such as occurring only at certain times of the day?

(c) How many signaling messages are trapped?

(d) Is there a relationship between fields matched by the trap and other fields in the signaling message?

(e) Are there other output messages or reports indicating the same type problem?

(f) Have the appropriate routing data audits and network tests been run?

Message Trap Limitations

(a) A maximum of five traps can be active at any given time with no more than one active trap per link. Together, all active traps may affect no more than 40 links at any given time.

(b) The rate at which trapped messages can be collected from the link nodes and sent to the 3B20D computer is limited by both computer and ring resources. Although the normal rate is much lower, an occasional burst of up to twenty 40-byte messages per second can be handled. Generally, more trapped messages can be captured at higher rates if fewer links have active traps or if trapped messages are smaller.

(c) The disk file can contain from 32 to 128 Kbytes of trapped message data (which is sufficient in most cases). After that limit is reached, data is overwritten, oldest data first.

(d) A trap is terminated when resources (such as memory or real time) either in the nodes or in the 3B20D computer are overloaded. A diagnostic message is printed out explaining the reason for the termination of the trap. A source-matched or returned message causes the trap to terminate immediately.

(e) The **OP:TRAP** output cannot be stopped once started or selected. Messages associated with a particular trap cannot be selectively printed.

Typical Message Trap Scenarios

11.35 Message trap can be used to:

(a) Aid in SS7 network fault isolation

(b) Provide network security.

11.36 Some possible uses are:

(a) Identify messages from a particular network using the OPC field.

(b) Identify messages to a particular switch using the DPC field.

(c) Isolate a problem to a particular region of a network by trapping on a specific set of links and analyzing trap data.

(d) Determine the cause of strange messages indicated in **REPT:DUMPMSG** output.

(e) Identify outgoing network management messages on particular links.

(f) Analyze messages that fail screening due to unknown destinations.

(g) Determine the source of messages with no GTT when failing translation at an STP.

(h) Determine the cause of screening failures and/or isolate potential network security problems by identifying nonsignaling-related data.

(i) Determine whether or not outgoing signaling messages are handled by certain link nodes in a switch when call processing is lost.

(j) Determine if SLTM/SLTA is exchanged during link initialization procedures.

Example Scenarios

EXAMPLE 1:

```
SET:TRAP,LNKLST=00-01-00-02-32-01-32-02:OPC=H'DC02FF,
MS=H'FFFF00:RATE=10,NOSAVE,ST=18-00;
```

When isolating faults in the SS7 network, specific routing problems can be identified by trapping on certain fields related to the routing of messages. In this example, an STP traps all incoming messages from a specific network identifier and cluster on specific links in the STP. Since this would generate many matched messages, trapping is at a rate of 1 out of 10 and does not start until 6 p.m.

EXAMPLE 2:

```
SET:TRAP,LNKR=32-00-48-00,MTYPE=SCCP:
RTDSP=N,SAVE,DUR=72-00;
```

At an *A-I-Net* products STP, a CNI measurement report indicates a large number of SCCP messages having no global title translation. A trap is set up for all locally originated SCCP messages. Since a large number of samples is necessary, the duration is set for several days and the data is saved on disk. The trap is activated immediately. The trapped messages are printed later and the global title field analyzed for patterns that may indicate the source of the problem.

EXAMPLE 3:

```
SET:TRAP,LNKSET=01,MTYPE=ALL7::RTDSP=Y,DEST=64;
```

Many miscellaneous screening failures are noted from Network ID=x. To determine the cause of the failures, a trap is set on linkset "01" (the only assigned screening linkset to network x) for all types of messages. The trapped messages are then printed and the message type field checked for "UNDEF7." Messages with this type are invalid and are analyzed to determine the cause of the screening failures. Since this may be a security problem, the trap is activated immediately and results are displayed on the ROP in real time.

EXAMPLE 4:

```
(PDS)
SET:TRAP,LNKSET 3,MTYPE MSPEC7 ; ;RATE 1,RTDSP Y,NOSAVE!
```

Example 4 will trap all incoming Signaling Link Test Messages (SLTM) or Signaling Test Message Acknowledgement (SLTA) messages on all links in linkset three in real time and not saved on disk.

EXAMPLE 5

```
SET:TRAP,LNKSET 3,MTYPE ISDN7, ;MODE OUT;
DPC X'FF1E02, MS X'FFFFFF, OFSTB (10,X'0100),
MS X' FF00, OFSTB (26, X' 695008), MS X'FFFFFF;
RATE 1,RTDSP Y, MGSZE 100!
```

Example 5 will trap IAMs to a point code, 255 028 002, with a called party number of 800-596-XXXX with a USI parameter for voice.

EXAMPLE 6:

```
SET:TRAP,LNKSET 3,MTYPE ISDN7, MODE OUT;
DPC X'FF1E03, MS X'FFFFFF, OFSTB (10,0100),
MS X'FF00, OFSTB (24, X'31454500), MS X'FFFFFF00;
RATE 1,RTDSP Y, MGSZE 60!
```

Example 6 will trap IAMs, with USI of 64-kb clear data, sent to point code 255 028 003 with a called number of 545-4132.

NOTE:
Network ID of 255 is fictitions.

12. LASS Screen List Editing and Validation Test Query

User Entry Through Screen List Editing

12.01 The LASS Screen List Editing (SLE) capability allows LASS Selective Feature (LSF) users to create and modify lists of telephone numbers associated with their (the user's) directory number (DN). These listed numbers are used to identify calling parties. Calls from a listed number are given special treatment by the LSFs. Each LSF has it own associated screening list for each user DN. The SLE access is available only to those customers subscribing to LSF.

12.02 The following LSFs are available in the 5ESS switch generic 5E6 and later software release and the 1A ESS switch generic 1AE11.03 and later software releases:

- Selective Call Acceptance
- Selective Call Forwarding
- Selective Call Rejection
- Selective Distinctive Alert
- Computer Access Restriction.

12.03 The LSF maximum list size global office parameter per feature (above list) may contain legal values ranging from 3 to 31. For example, **Glcarmx** (CARMAXSIZE) may contain a value of 3 while the parameter associated with Selective Call Forwarding (SCF) may be set to 15. These values are provided to control the maximum number of entries a subscriber may have per screening list and per feature. In generic software release 5E6, these parameters are changeable through RC View 8.21. In generic software release 1AE11.03, these values are controlled by set cards.

12.04 A LASS user can add a 7- or 10-digit telephone number to a screening list after the number or centrex extension passes certain validation checks. All telephone numbers added by the LASS user to the screening lists are validated by SLE to ensure that calls are correctly screened (unassigned DNs are not allowed on the list). For numbers not assigned at the user's switch, an SS7 TCAP query may be made of the switch where the number is assigned. If no checks fail, the number is added to the screening list and a confirmation announcement is returned to the user. If the entry fails, an announcement is sent to the user and the number is not added to the screening list.

NOTE:
An office parameter in the 5ESS switch (field **"VALIDATE LSF ENTRY"** in RC View 8.21) determines whether an SS7-TCAP query is made.

12.05 Telephone company switching office personnel have the capability to build, change, delete, list, and activate or deactivate features for all LASS Selective Features (LSFs) via a service order. The telephone company can use a service order when the LSF user is having trouble with the Screen List Editing (SLE) or for LSF users with direct connect lines, manual lines, and denied originating treatment lines. Attendants and multiparty lines cannot be assigned LSFs.

12.06 List entries entered by service order cannot be validated when they are entered, since SLE is the only source of the validations. Entries can be validated prior to executing the service order through the use of the **OP:LASSRQST** input message and the results contained in the **OP:LASSRQST** output message. It is strongly recommended that the input message be used to validate the number(s) in order to weed out errors and invalid DNs or lines types. Entering this message invokes the same validation checks executed by the LASS-SLE. Diagnostic information is returned to the ROP in the **OP:LASSRQST** message, to indicate the source(s) of error, or successful validation. This tool is available on 5ESS switch generic 5E6 and later software releases, and on 1A ESS switch generic 1AE11.06 and later software releases.

NOTE:
The details of the above input and output messages may be found in 235-600-700, "*5ESS Switch Output Messages*", IM-6A001-01, "*1A ESS Input Message Manual*", and OM-6A001-01, "*1A ESS Output Message Manual.*" Additional information concerning this LASS feature may be found in 235-190-130, "*5ESS Switch Local Area Signaling Service Feature Document*", and 231-390-235, "*1A ESS LASS Common Channel Signaling System 7—General Description.*"

12.07 The **OP:LASSRQST** input message may also be used as a test to verify LASS-TCAP connectivity to another office (refer to Table 6-A).

13. ASP Test Query

13.01 This tool requests that an Advanced Services Platform (ASP) test query be sent in order to determine call routing treatment provided by an SCP data base. Only an ASP Service Switching Point (SSP) can originate this test query.

13.02 This tool is available for the following products and is documented as listed below:

Product	Document
5ESS	235-600-700, *5ESS Input Manual* 235-600-750 *5ESS Output Manual* for the correct format of the **TST:ASP** or **TST:ASPTQ** input and output messages
1A ESS	IM-6A001, *1A ESS Input Manual* *OM-6A001, 1A ESS Output Manual* for the correct format of the **TEST:ASP** input and output messages
4ESS	IM-4A000 (or 4B000), *4ESS Switch Input Message Manuals* for the correct format of the **TEST:TCAPAIN** input & output messages.

Also refer to Table 6-A.

13.03 The SCP response may:

(a) Contain ASP SSP routing information such as a directory number, carrier identification code, route index, route type, call treatment indication, billing indication, and/or an Automatic Call Gap (ACG).
(b) Request the ASP SSP to play an announcement and/or collect more digits.
(c) Indicate a query failure.
(d) Indicate a query rejection.
(e) Return an error.
(f) Indicate a time-out.

13.04 This tool reports the SCP response and does not guarantee that the ASP SSP has been properly provisioned to carry out the SCP instructions. A successful response from the SCP will imply that initial SS7 routing translations (that is, global title translations) are properly provisioned in the ASP SSP.

CAUTION:
If the SCP response requests more digits be collected [that is, a Personal Identification Number (PIN)] by the ASP SSP and returned to the SCP before appropriate routing instructions can be given, SS7 routing translations in the ASP

SSP must be provisioned for MTP routing to the SCP point code. This is accomplished by using 5ESS Switch RC view 15.9 to define SS7 routing to the SCP's network identifier and cluster number.

14. Service Switching Point/800 Test Query

Purpose

14.01 The Service Switching Point (SSP/800) test query verifies the integrity of the SS7 network and the consistency of CNI, Signaling Transfer Point (STP), and Service Control Point (SCP) data.

14.02 A test message is input which contains a 10-digit SSP number, a 3-digit or 10-digit Automatic Number Identification number of the calling party, a 3-digit Local Access and Transport Area (LATA) number, and (optionally) an originating station type. The message causes a Transaction Capabilities Application Part (TCAP) query to be sent from the switch to the SCP via one or more STPs. If the query is successful (that is, the SSP test message is successfully routed to the SCP and the response successfully routed to the switch), an output message is printed. If the query is not successful (for example, time-out), an error message is printed.

14.03 The origination station type is not an optional input parameter for the 1A ESS switch. If it is not input, the input message SSP-EIGHT will receive an NG tack, and the Test Query will not be sent to the SCP.

NOTE:
This message should be used to verify the data before making test calls.

14.04 Refer to Table 6-A for the appropriate IM/OM for the test message to be input.

Special Consideration

14.05 The test itself does not validate that the appropriate trunk routing has been provisioned to route the call. It simply queries the translations in the SCP data base and reports its findings to the test initiator. In querying the SCP, a successful test response will indicate that the SS7 routing translations are correctly provisioned along the SS7 test path.

15. Calling Card Test Query

15.01 The Calling Card (CCRD) test query verifies the integrity of the SS7 network and the consistencies of CNI, *A-I-Net* products STP, *A-I-Net* products SCP, and Line Information Data Base (LIDB) data.

15.02 A test message input that contains the 14-digit calling card number to be queried, a 10-digit back number, and a 10-digit called Directory Number (DN). The message causes a Transaction Capability Application Part (TCAP) query to be sent from the switch to an LIDB via an SCP and one or more STPs. If the query is successful (routed to the LIDB and the response successfully routed to the switch), an output message is printed. The output message may also indicate the query cut back level (0-7 out of 8 being cut back) and Regional Accounting Office (RAO).

NOTE:
This test query should be used to verify data before making test calls.

15.03 Refer to Table 6-A for the appropriate IM/OM test message to be input.

A. Special Consideration

15.04 The test itself does not validate that the correct routing has been provisioned for DN. However, it does verify the CCRD Number (including PIN), Service Screening, Data base Congestion Level, Network Conditions (blocked, overload, routing data to LIDB), and validate Billing for DN. In querying the LIDB, a successful response verifies the SS7 routing along the test path and the existence of the destination LIDB (failure is "CCIS FAILURE—DESTINATION NOT EQUIPPED").

Miscellaneous Engineering Considerations

7

Contents Page

Miscellaneous Engineering Considerations

7

1. Switch Replacement

1.01 A switch may be retired for any of a number of reasons. Among these reasons are resource exhaustion, technological advancement, and new service offerings. Two alternatives exist when the switch retires:

(1) Replace it with a new switch.

(2) Move its lines and trunks to an existing switch.

1.02 In the past, replacing a 1A ESS™ switch currently using SS7 with a 5ESS® switch using SS7 service required the Local Exchange Carrier to follow a manual process to test not only SS7 trunks that are reused in the 5ESS switch, but also SS7 trunking growth. This process is time consuming, expensive, and potentially error-prone.

1.03 To expedite and simplify this replacement process, a feature known as Pseudo Point Code Capability (PPCC) is available.

1.04 The PPCC provides the ability to assign a temporary point code to the 5ESS switch to facilitate trunk testing and call processing in the interval before replacement of the 1A ESS switch. It also allows the reuse of the 1A ESS switch point code in an installing 5ESS switch. For further information about PPCC, contact your Lucent Technologies Account Representative.

2. Signaling Link Rehome Procedure

2.01 The following is a Signal Transfer Point (STP) rehoming procedure for Lucent Technologies switching products in the Local Exchange Carrier marketplace. The switch in question is to be rehomed from STP mated pair **AB** to STP mated pair **CD** (Figure 7-1). For the purposes of this procedure, linkset "**a**" connecting the switch with STP **A** is rehomed to STP **C**. Linkset "**b**" connecting the switch with STP **B** is rehomed to STP **D**. Likewise, combined linkset **C** is rehomed from STPs **A** and **B** to STPs **C** and **D**.

NOTE:
The designation of EVEN/ODD STPs must be maintained after the rehoming procedure is complete. Let STP **A** be designated as the EVEN STP. After the procedure, STP **C** must be designated as the EVEN STP. The same holds true if STP **B** is designated as the ODD STP. After the procedure, STP **D** must be designated as the ODD STP.

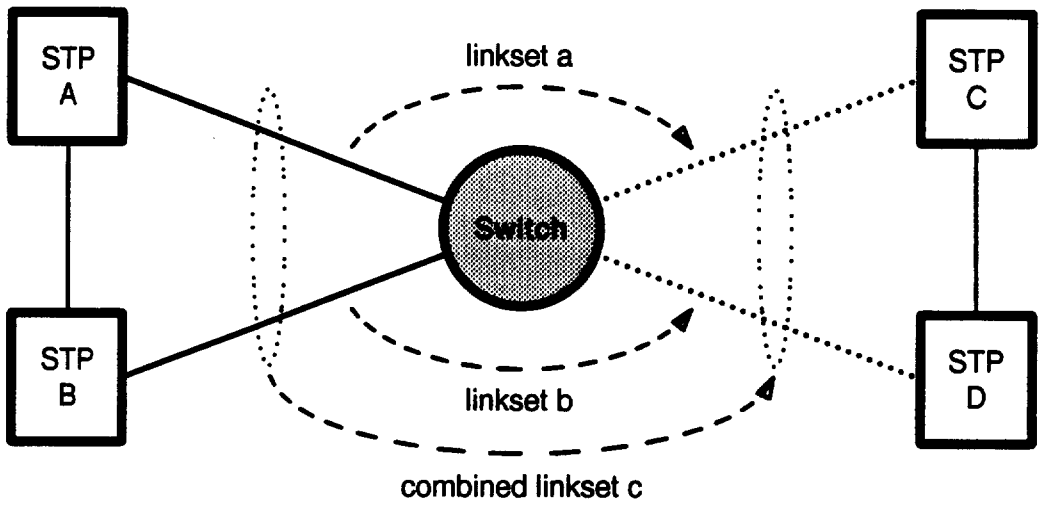


Figure 7-1. Rehoming Switch from One STP Mated Pair to Another

NOTE:
The procedure makes the assumption that "**B**" or "**D**" signaling links connect STP mated pair **AB** to STP mated pair **CD**. Before beginning this procedure, the telco must determine which STP mated pair will be performing the Global Title Translations (GTTs) for the switch following the rehoming procedure.

The SLK rehoming procedure is as follows:

(1) Activate the Signaling Link (SLK) monitor to observe activity on all SLKs. Enter one of the following:

MON:SLK ALL;ON (for 1A ESS Switch or 4ESS™ Switch)

MON:SLK=ALL:ON (for 5ESS Switch)

(2) Verify the current routing status within the switch. Enter one of the following:

OP:C7NET:PRTE (for 1A ESS Switch or 5ESS Switch)

OP:C7NET:ROUTING (for 4ESS Switch)

The Preferred Route (PREF RTE) and Active Route (ACT RTE) to STPs **A** and **B** should indicate as follows:

1AP3F, 5E9, and 4AP12	ROUTING FLAG	ACT LS	STATUS PRIM	ALT1	ALT2
STP A	UPOPCLU	a	aA	bA	
STP B	UPOPCLU	b	bA	aA	

WARNING:
Do not proceed with this procedure if the routing data is not as shown in subparagraph 2.01 (2). You must take the necessary corrective action to ensure all routing is allowable.

(3) Inhibit automatic removal of the Link Nodes for diagnostics on declare failures. Enter one of the following:

INH:DMQ;SRC ARR (for 1A ESS Switch or 4ESS Switch)

INH:DMQ;SRC=ARR (for 5ESS Switch)

(4) Change all SLKs in linkset "**a**" to STP **A** to the Manual Out Of Service (MOOS) state. For each SLK in linkset "**a**", enter one of the following:

CHG:SLK (xx,y);MOOS (for 1A ESS Switch or 4ESS Switch)
CHG:SLK=xx,y:MOOS (for 5ESS Switch)

WARNING:
If an SLK cannot be placed in the MOOS state, determine the reason for refusal and take the necessary corrective action.

(5) Verify the current routing status within the switch. Enter one of the following:

OP:C7NET:PRTE (for 1A ESS Switch or 5ESS Switch)
OP:C7NET:ROUTING (for 4ESS Switch)

The Preferred and Active Route indicators to STPs **A** and **B** should appear as follows:

1AP3F, 5E9, and 4AP12	ROUTING FLAG	ACT LS	STATUS PRIM	STATUS ALT1	STATUS ALT2
STP A	UPOPCLU	b	aP	bA	
STP B	UPOPCLU	b	bA	aP	

(6) Allow SLK recent changes to be made on the SLKs to STP **A** by first making the SLKs in linkset "**a**" unavailable as shown in Table 7-A.

Table 7-A. Changing SLK to STP

Switch	Function/View	Field
1A ESS™	LKDATA	MAJOR = unavailable
4ESS™	LKDATA	MAJORSTATE = unavailable
5ESS®	15.2	MAJORSTATE = UNA

(7) Change the STP routing information for link set "**a**" to route to STP **C** instead of STP **A**. First, delete the routing data to STP **A** shown in Table 7-B.

Table 7-B. Changing STP Routing Information

Switch	Function/View	Fields
1A ESS™	ROUTE	NTWK = STP A's network identifier CLUSTER = STP A's cluster LINKSET = "a" STP = y
4ESS™	LSROUT	CLUSTERID = STP A's cluster LINKSET = "a"
5ESS® 15.9, (5E9)	CLUSTER = STP A's cluster	ROUTING FLAG = UPOPCLU PRI ROUTE = "a"

(8) For each SLK in link set "**a**", change the SLK's Far-End Point Code (FEPC) and Far-End CLLI Code (FECLLI) from STP **A** to STP **C** as shown in Table 7-C.

Table 7-C. Changing FEPC and CLLI Codes

Switch	Function/View	Fields
1A ESS™	LKDATA	FAR END POINT CODE = *FEPC* FAR END CLLI CODE = *FECLLI*
4ESS™	LKDATA	FAR END PINT CODE = *FEPC* FAR END CLLI = *FECLLI*
5ESS®	15.2	FAR END PNT CODE = *FEPC* FAR END CLLI = *FECLLI*

(9) Once the routing data for STP **A** has been deleted, add the routing data for STP **C** as shown in Table 7-D. The routing type used should correspond to linkset routing.

Table 7-D. Adding Routing Data for STP

Switch	Function/View	Fields
1A ESS™	ROUTE	NTWK = STP C's network identifier CLUSTER = STP C's cluster LINKSET = "a" STP = y
4ESS™	LSROUT	CLUSTERID = STP C's cluster LINKSET = "a"
5ESS®	15.9 (5E9)	CLUSTER = STP C's cluster ROUTING FLAG = UPOPCLU PRI ROUTE = "a"

(10) Since you still want to be able to route to STP **A** for the purposes of Global Title at this point, it is necessary to add back the cluster-level routing data for STP **A** (Table 7-E). Routing is to be done over the combined linkset. This step makes the assumption that **B** or **D** links exist and are in service between STP pairs **AB** and **CD**. If this is not the case, the Common Network Interface (CNI) data base must be updated with the correct STP pair for each GTT type defined (refer to Step 18 for the appropriate messages/views).

Table 7-E. Adding Cluster-Level Routing Data for STP

Switch	Function/View	Fields
1A ESS™	ROUTE	NTWK = STP A's network identifier CLUSTER = STP A's cluster LINKSET = "c" STP = y
4ESS™	CLSROUT	CLUSTERID = STP A's cluster LINKSET = "c"
5ESS®	15.9 (5E9)	CLUSTER = STP A's cluster FLAG = UPOPCLU LINKSET = "c"

(11) Make the first SLK in linkset "**a**" available by changing the SLK's Major State to available as shown in Table 7-F. If there is more than one SLK in linkset "**a**", only the first SLK is made available so that you can prove-in that SLK and thus make sure the changes are made correctly. Once it is determined that one SLK is working correctly, the others are put into service.

Table 7-F. RC View Functions—Changing MAJOR State

Switch	Function/View	Field
1A ESS™	LKDATA	MAJOR = available
4ESS™	LKDATA	MAJORSTATE = available
5ESS®	15.2	MAJORSTATE = AVL

(12) Physically relocate the SLKs in linkset "**a**" from STP **A** to STP **C**.

(13) Restore the first SLK in linkset "**a**" to service. Enter one of the following:

CHG:SLK (xx,y);IS (for 1A ESS Switch or 4ESS Switch)

CHG:SLK=xx,y:IS (for 5ESS® Switch)

Observe that the MON:SLK "LEVEL 2 COMPLETE" message or "PROVE-IN COMPLETE" message appears. The SLK indicators should reflect that the SLK is in service.

(14) Verify the current routing status within the switch. Enter one of the following:

OP:C7NET:PRTE (for 1A ESS Switch or 5ESS Switch)

OP:C7NET:ROUTING (for 4ESS Switch)

The Preferred and Active Route indicators to STPs **A**, **B**, and **C** should appear as follows:

1AP3F, 5E9, and 4AP12	ROUTING FLAG	ACT LS	STATUS PRIM	ALT1	ALT2
STP C	UPOPCLU	a	aA		
STP B	UPOPCLU	b	bA		

(15) At this point in the procedure the switch is communicating with STPs **B** and **C** as reflected in Figure 7-2.

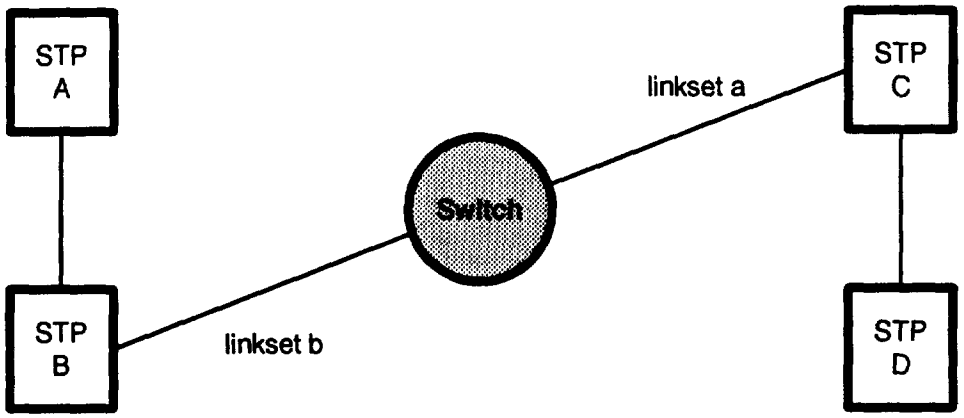


Figure 7-2. Communication Prior to Activating All SLKs

Before activating the remaining MOOSed SLKs (if any exist) in linkset "**a**", it is advisable to test that the switch is routing to STP **C** properly. To do this, physically fail all SLKs in linkset "**b.**" An easy way of doing this is to locally loop back linkset "**b**"'s data set(s).

Once the SLKs in linkset "**b**" are failed, make test calls.

Once you are satisfied that the switch is routing properly through linkset "**a**", reactivate the SLKs in linkset "**b**" (that is, remove the local loopback).

(16) Restore the remaining SLKs (if any exist) in linkset "a." For each SLK in the MOOS state, enter one of the following:

CHG:SLK (xx,y);IS (for 1A ESS™ Switch or 4ESS Switch)

CHG:SLK=xx,y:IS (for 5ESS Switch)

(17) Rehome linkset "**b**" from STP **B** to STP **D** by repeating Steps 4 through 16 using (where applicable):

- — Linkset "**b**" instead of linkset "**a**"
- — Linkset "**a**" instead of linkset "**b**"
- — STP **B** instead of STP **A**
- — STP **D** instead of STP **C**.

(18) At this point in the procedure the switch should be communicating with STPs **C** and **D** as reflected in Figure 7-3.

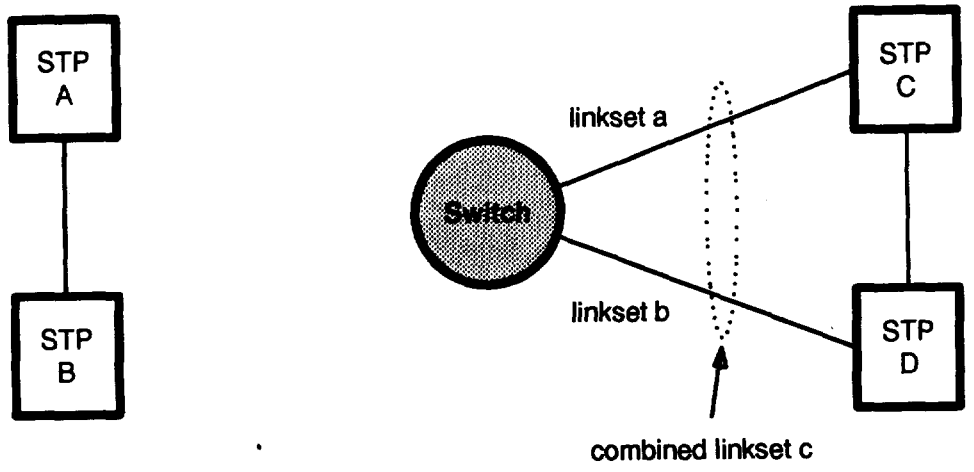


Figure 7-3. Switch With New Home STP Pair

If Global Title is to be performed by STP pair **CD** instead of STP pair **AB**, each GTT type must be updated to reflect this as shown in Table 7-G. It is strongly recommended that a capability code for STP pair **CD** be used rather than the individual STP point codes.

Table 7-G. Updating GTT Types

Office	Function/View	Fields
1A ESS™ Switch	RC:CNI;CHG GBLTT	TRANTYPE = defined GTT type STP0 = capability code of STP pair CD STP1 = capability code of STP pair CD
4ESS™ Switch	GTTRAN	TRANSLATION TYPE = defined GTT type EVEN STP PC = capability code of STP pair CD ODD STP PC = capability code of STP pair CD
5ESS® Switch*	15.11	TRANSLATION TYPE = defined GTT type PC 1 = capability code of STP pair CD PC 2 = capability code of STP pair CD

*As a minimum, the 5ESS Switch general translator translation type (that is, 256) must be the updated local STP pair CD.

(19) Verify the current routing status within the switch. Enter one of the following:

OP:C7NET:PRTE (for 1A ESS Switch or 5ESS Switch)

OP:C7NET:ROUTING (for 4ESS Switch)

The Preferred and Active Route indicators to STPs **B** and **C** should appear as follows:

1AP3F, 5E9, and 4AP12	ROUTING FLAG	ACT LS	STATUS PRIM	STATUS ALT1	STATUS ALT2
STP C	UPOPCLU	a	aA	bA	
STP D	UPOPCLU	b	bA	aA	

(20) Allow automatic removal of the Link Nodes for diagnostics on declare failures. Enter one of the following:

ALW:DMQ;SRC ARR (for 1A ESS Switch or 4ESS Switch)

ALW:DMQ;SRC=ARR (for 5ESS Switch)

(21) Turn the SLK monitor off. Enter one of the following:

MON:SLK ALL;OFF (for 1A ESS Switch or 4ESS Switch)

MON:SLK=ALL:OFF (for 5ESS Switch)

3. Transmission Capabilities on SLC®, D4, and D5 Carriers

3.01 The following information is provided to assist in the identification of transmission problems involved with Incoming Calling Line Identification (ICLID) data when an SLC carrier facility is in the path. The basic requirement for any Digital Loop Carrier (DLC) arrangement that supports Local Area Signaling Service (LASS) offerings is that the channel units must provide for *On-Hook Transmission* (OHT). That is, the channel units must be able to pass signaling information to the station set when the receiver is in the on-hook condition. In general, LASS offerings can be supported on Lucent Technologies SLC® 96 and SLC Series 5 Carrier Systems, but certain plug-in codes and combinations are required. Table 7-H addresses the issue of compatibility for SLC 96 and SLC Series 5 Carrier System remote terminations with the 5ESS switch. The SLC 1 and SLC 40 Carrier Systems are not compatible with ICLID OHT.

Table 7-H. SLC Carrier Compatibility with OHT of ICLID Data

CO Termination		SLC® 96 Carrier Remote Termination				
		WP20	WP20B	WP20C	WP20D	WP37
SLC 96 Carrier	WP10	Y	Y	Y	Y	Y
	WP10B	Y	Y	Y	Y	Y
	WP10C	Y	Y	Y	Y	Y
	WP10D	Y§	Y§	Y§	Y§	Y§
	WP36	Y	Y	Y	Y	Y†
SLC Series 5 Carrier	AUA31					
	AUA32					
	AUA38					
	AUA39					
INTEGRATED		Y§	Y§	Y§	Y§	Y§

CO Termination		SLC Series 5 Carrier*			
		AUA25	AUA51	AUA58	AUA59
SLC 96 Carrier	WP10	Y	N	Y	Y
	WP10B	Y	N	Y	Y
	WP10C	Y	N	Y	Y
	WP10D	Y§	N	Y§	Y§
	WP36	Y†	N	Y§	Y†
SLC Series 5 Carrier	AUA31	N	N	N	N
	AUA32	N	N	N	N
	AUA38	Y§	N	Y§	Y§
	AUA39	N	N	Y§	N
INTEGRATED		Y§‡	N	Y§	Y§‡

Legend

Y—Compatible usage for ICLID/OHT support.

N—Not compatible for ICLID support.

* Also supports distinctive ringing (in both Start and Ground Start Modes).

† Use with ICLID/OHT only in Loop Start Mode (do not use in Ground Start Mode).

‡ ICLID/OHT only when entered in the switch data base as Plain Old Telephone Service (POTS) (feature does not work if entered as Special Plain Old Telephone Service (SPOTS).

§ Channel unit also supports 2-way OHT (suitable for remote meter reading, etc.); however, specific features also need to be implemented in the switch.

3.02 Table 7-I provides a D4, D5 Foreign Exchange Office-Foreign Exchange Station (FXO-FXS) channel unit pairing evaluation for the ICLID feature and FSX customer loop validation. Table 7-I shows an analysis results for On-Hook Transmission Loss Increase Toward Station (OTLTS) in reference to Off-Hook or circuit design loss values.

Table 7-I. ICLID Hardware Compatibilities and Loss Calculations

FXO D4, D5 Hardware	FXO OTLTS	FXS D4, D5 Hardware (1)	FXO OTLTS	FXO +FXS OTLTS	ICLID Compatible w/21Kft 26NL & 125A/B CPE	ICLID (5)* Loss w/23 dBrnC & 20 dB S/N
J98726BE J98726BK J98726SK	3 dB	J98726BD J98726BL AEK20 AEK20B, Series 1,2	0 dB	3 dB	Yes (4)	24.4 dB 18.5 dB (7)
AEK21B (3)	11 dB			11 dB	Yes	18 dB
J98726BE J98726BK J98726SK	3 dB	AEK20B Series 3 AEK20C	9 dB	12 dB	Yes	18.5 dB (7) 12.5 dB
AEK21B (3)	11 dB			20 dB	No	10.5 dB 4.5 dB (7)
J98726BE J98726BK J98726SK	3 dB	J98726SG-3, List 3 (2)	15 dB	18 dB	Yes	Fixed 4.0 dB design loss (6)
AEK21B (3)	11 dB			26 dB	Yes	

* Numbers in parentheses () identify the appropriate NOTE for that item.

NOTE 1:
All D5 gain-transfer (CNs [FXS 6 and 7]) regardless of hardware, cuts off transmission toward station. Loss shown is for nongain-transfer function (FXS [A, B, C, D,]).

NOTE 2:
D4 J98726SG-1,-2 hardware prior to J98726SG-3, List 3 (current production) cuts off transmission toward the station.

NOTE 3:
Applies to all D5 FXO FCNs including gain-transfer. All AEK21 hardware distorts transmission on-hook.

NOTE 4:
Derived using nominal 1.5-dB minimum design loss (1.0 for 4-wire gain stability plus 0.5 office wiring) recommended for nongain transfer channel unit pairs. If standard FX line design of 4.0-dB loss are observed, maximum loop loss is limited to 2.5 dB.

NOTE 5:
The ICLID loss is at 2800 Hz. Loss shown is remaining loss available after channel units on-hook losses are accounted for. Computation uses present 125B sensitivity (-50 dBm and 2800 Hz); assumes 20-dB Signal-to-Noise (S/N) [Lucent Technologies Voice Band Data Objective is 24] margin and 23-dBrnC noise threshold criteria at the 125A/B CPE. The range is decreased (increased) a dB for each dB S/N margin that is increased (decreased) or for each dB the 23-dBrnC noise level threshold is increased (decreased). Currently there is no specification that really defines what the 125A/B S/N margin or sensitivity requirement should be.

NOTE 6:
Assumes the overall end-to-end circuit loss using gain-transfer units should be essentially flat (equalized) and typically limited to a fixed circuit design value of 4 dB.

NOTE 7:
Range with 25-dBrnC noise threshold and 24-dB S/N margin.

Acronyms

8

1. Introduction

1.01 The following is a list of definitions for the acronyms used in this document. For a list of reference documents, see Chapter 9. This information is intended to help ensure uniformity in Local Exchange Carrier (LEC) Common Channel Signaling System 7 (CCS7) network documentation.

2SCCS	No. 2 Switching Control Center System
30MPR	Thirty Minute Marginal Performance Report
3BI	3B Interface
ABSBH	Average Busy Season-Busy Hour
AC	Automatic Callback
ACC	Automatic Congestion Control
ACCL	Automatic Congestion Control Level
ACG	Automatic Call Gapping
ACM	Address Complete Message
ACNR	Application Critical Node Restore
ACRT	Administration CRT
ACT	Active
ACT RTE	Active Route

AIM	Application Integrity Monitor
ALSR	Alternate A-Linkset Routing
AM	Administrative Module
ANI	Automatic Number Identification
ANSI	American National Standards Institute
AP	Attached Processor
API	Attached Processor Interface
APS	Attached Processor System
AR	Automatic Recall
ARR	Automatic Ring Recovery
ASE	Application Service Element
ASP	Advanced Services Platform
ASUR	Application Specified Unconditional Restore
AT	Access Tandem
ATP	All-Tests-Pass
ATP	Access Transport Parameters
AVL	Available
BCLID	Bulk Calling Line Identification
BISO	Beginning of Isolation
CAR	Computer Access Restriction
CATP	Conditional All-Tests-Pass
CBA	Change Back Acknowledgement
CCIS6	Common Channel Interoffice Signaling 6
CCITT	International Telegraph and Telephone Consultative Committee
CCME	CCS7 Continuity Check Modification Enhancement
CCRD	Calling Card
CCS	Common Channel Signaling
CCS7	Common Channel Signaling System 7
CCT	Continuity Check Transceiver

CDPD	Called Party Address
CDX	Compact Digital Exchange
CIC	Circuit Identification Code
CIN	Circuit Identification Number
CLS	Combined Linkset
CLU	Cluster
CNAM	Calling Name Identification
CNI	Common Network Interface
CNIINIT	CNI Initialization
CNR	Critical Node Recovery
COEES	Central Office Equipment Engineering System
COND	Conditional
COT	Continuity Test, Customer Originated Trace
CPE	Customer Premises Equipment
CPI	Circuit Program Index
CPN	Calling Party Number
CPNP	Calling Party Number Presentation
CPNPC	Calling Party Number Presentation Capability
CQA	Circuit Query Allowed
CRA	Circuit Restoration Acknowledgment Message
CRC	Cyclic Redundancy Check
CTAM	Customer Technical Assistance Management Center (Customer/Product Hotline)
CU	Control Unit
CVR	Circuit Validation Response
CVT	Circuit Validation Test
DA	Distinctive Alerting
DCIS6	Destination Common Channel Interoffice Signaling 6
DDSBS	Duplex Dual Serial Bus Selector
DFA	Digital Facility Access

DGN	Diagnose Diagnostic
DL	Digital Loopback
DLC	Digital Loop Carrier
DLN	Direct Link Node
DMA	Direct Memory Access
DMS	Data Base Management System
DN	Directory Number
DP	Dial Pulse
DPC	Destination Point Code
DS	Digital Signal
DSU	Digital Service Unit
DTE	Data Terminal Equipment
EA	Equal Access
EAEO	Equal Access End Office
EAMF	Equal Access Multifrequency
EAR	Error Analysis and Recovery
EAS	Equal Access Signaling
ECD	Equipment Configuration Data Base
ECIS6	Embedded Common Channel Interoffice Signaling 6
EECT	End-to-End Call Trace
EISO	End of Isolation
EO	End Office
ETC	End Office Access Tandem Connecting
FECLLI	Far-End CLLI Code
FEPC	Far-End Point Code
FHC	Final Handling Code
FLTY	Faulty
FTSP	Final Translation Signaling Point
FX	Foreign Exchange

FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
GT	Global Title
GTSR	Gateway Traffic Summary Report
GTT	Global Title Translation
GTXTAB	Global Title Translation Table
HDBH	High-Day Busy Hour
IAM	Initial Address Message
IC	Interexchange Carrier
ICC	Incoming Circuit
ICL	Inserted Connection Loss
ICLID	Individual Calling Line Identification
ID	Identification
IEC	Interexchange Carrier
IFB	Interframe Buffer
IM	Input Message
IMS	Interprocess Message Switch
INC	Incoming
INIT	Initializing
I/O	Input/Output
IS	In-Service
ISC	Incoming Signaling Characteristics
ISDN	Integrated Services Digital Network
ISO	Isolated
ISUP	Integrated Service Digital Network - User Part
ISUPC	International Signaling Point Code
ITSP	Intermediate Translation Signaling Point
IUN	IMS User Node
IXC	Interexchange Carrier

LASS	Local Area Signaling Services
LATA	Local Access and Transport Area
LCLT	Local Tone/Announcement Indicator
LDL	Local Digital Loopback
LEC	Local Exchange Carrier
LED	Light Emitting Diode
LIDB	Line Information Data Base
LL	Local Loopback
LN	Link Node
LOCP	Local Point Code
LPOPC	Local Populated Cluster
LS	Linkset
LSF	LASS Selective Feature
LSF	Line Switch Frame
LSSU	Link Status Signal Unit
MAN	Manual operation
MC0	Machine Congestion Level 0
MC1	Machine Congestion Level 1
MC2	Machine Congestion Level 2
MC3	Machine Congestion Level 3
MCRT	Maintenance Terminal
MF	Multifrequency
MML	Man-Machine Language
MOCT	Measurement Output Control Table
MOOS	Manual Out-of-Service
MPR	Machine Performance Report
MRVA	MTP Routing Verification Acknowledgment
MRVR	MTP Routing Verification Result
MRVT	MTP Routing Verification Test
MS	Mask

MSR1	Machine Service Report, Part 1
MSR2	Machine Service Report, Part 2
MSU	Message Signal Unit
MTP	Message Transfer Part
NAP	Network Access Point
NAUD	Node Audit
NCA	No Circuit Available
NCP	Network Control Point
NI	Network Interconnect
NID	Network Identifier
NNAUD	Neighbor Node Audit
NOC	Normalized Office Code
NORM	Normal Operation
NP	Node Processor
NPA	Numbering Plan Area
NSFI	Next Screening Function Indicator
NSPMP	Network Switching Performance Measurement Plan
NSRI	Next Screening Reference Index
NT	No Token
OA&M	Operational, Administrative, & Maintenance
OAT	Originating Access Tandem
OCC	Other Carrier Connecting
ODA	Office Data Assembly
ODD	Office Dependent Data
OD4NAT	OD4 Network Announcement Table
OEO	Originating End Office
OFSTB	Office Byte
OGC	Outgoing Circuit
OHT	On-Hook Transmission

OM	Output Message
OMAP	Operations, Maintenance, and Administration Part
OOS	Out-of-Service
OPC	Originating Point Code
ORG	Originated
OS	Operating System
OSC	Outgoing Signaling Characteristics
OSS	Operations Support Systems
OTLTS	On-Hook Transmission Loss Increase Toward Station
OTO	Originating Toll Office
PC	Point Code
PCF	Point Code Format
PCP	Per-Call Privacy
PDS	Program Documentation Standards
PIN	Personal Identification Number
PMCR	Plant Measurements Common Report
POTS	Plain Old Telephone Service
PPC	Primary Point Code
PPCC	Pseudo Point Code Capability
PSLT	Periodic Signaling Link Test
PTS	Per-Trunk Signaling
QUSBL	Quarantine Usable
RAC	Ring Access Circuit
RAO	Regional Accounting Office
RC	Recent Change
RCPTP	Recent Change for Protocol Timers and Parameters
RDB	Routing Data Block
RDL	Remote Digital Loopback
REL	Release message

RFR	Reason for Return
RI	Ring Interface
RI0	Ring Interface 0
RI1	Ring Interface 1
RLC	Release Complete
RLS	Release
RNA	Ring Node Address
ROP	Receive Only Printer
RPC	Ring Peripheral Controller
RPCN	Ring Peripheral Controller Node
RPOPC	Remote Populated Cluster
RTR	Real-Time Reliable
SCA	Selective Call Acceptance
SCCP	Signaling Connection Control Part
SCF	Selective Call Forwarding
SCS	Service Circuit Switch
SCP	Service Control Point
SCR	Selective Call Rejection
SIM	System Integrity Monitor
SEC	Switching Equipment Congestion
SIO	Service Information Octet
SIPO	Signaling Indication Processor Outage
SLE	Screen List Editing
SLK	Signaling Link
SLS	Signaling Link Selection
SLT	Signaling Link Test
SLTA	Signaling Link Test Acknowledgment
SLTM	Signaling Link Test Message
SM	Switching Module
SMAP	System Management Application Process

S/N	Signal-to-Noise
SNM	Signaling Network Management
SNPR1	Signaling Network Performance Report, Part 1
SNPR2	Signaling Network Performance Report, Part 2
SPC	Secondary Point Code
SPI	Signaling Point Isolation
SPOTS	Special Plain Old Telephone Service
SRSCT	Signaling Route Set Congestion Test
SRST	Signaling Route Set Test
SRVA	SCCP Route Verification Acknowledgment
SRVR	SCCP Route Verification Result
SRVT	SCCP Route Verification Test
SSI	Subsystem Allowed
SSD	Second Start Dial
SSI	Small Scale Integration
SSN	Subsystem Number
SSP	Service Switching Point
SSP	Subsystem Prohibited
SST	Subsystem Status Test
SS7	Signaling System 7
STAR	Simultaneous Trunk Conversion via Automatic Recent Change
STD	Standard
STBY	Standby
STP	Signaling Transfer Point
SU	Signaling Unit
T&M	Testing and Maintenance
T/A	Tone/Announcement
TAN	Trunk Appearance Number
TAT	Terminating Access Tandem
TCAP	Transaction Capabilities Application Part

TCC	Trunk Class Code
TCIC	Trunk Circuit Identification Code
TDA	Translation Data Assembly
TEO	Terminating End Office
TFA	Transfer Allowed
TFC	Transfer Control
TFN	Traffic Network Number
TFP	Transfer Prohibited
TFR	Transfer Restricted
TG	Trunk Group
TNN	Trunk Network Number
TOPAS	Testing Operations Provisioning and Administration System
TOT	Type of Trunk
TPC	Translation Point Code
TSG	Trunk Subgroup
TSP	Translation Signaling Point
TT	Translation Type
UCR	Unidentified Call Rejection
UDTS	Unitdata Service
UNAV	Unavailable
UNEQ	Unequipped
UNTSTD	Untested
USBL	Usable
VER	Verify
VPA	Voice Path Assurance

References

9

Contents Page

References

9

1. Introduction

1.01 Following is a list of documents related to Signaling System 7 (SS7) operations, administration, and maintenance. Many of these are also referenced in the descriptions in this manual.

- 231-301-302, *Common Channel Signaling System 7, Trunk Maintenance, 2-Wire, 1A ESS™ Switch*
- 231-318-334, *Trunk Translation Recent Change Formats (1AE8A.05 Through 1AE10 Generic Programs), 1A ESS Switch*
- 231-318-340, *Local Area Signaling Services (LASS), Recent Change Implementation Procedures (1AE9 and Later Generic Programs), 1A ESS Switch*
- 231-318-375, *Common Channel Signaling System 7, Recent Change Implementation Procedures and Trunk Conversion (1AE10.01 and Later Generic Programs), 1A ESS Switch*
- 231-318-376, *Common Channel Signaling System 7, Service Switching Point (SSP), Translation Implementation Procedures (1AE10.01 and Later Generic Programs), 1A ESS Switch*
- 231-361-026, *Common Channel Signaling System 7, CNI Ring Implementation Guide, 1A ESS Switching System*
- 231-368-020, *1A ESS Switch, Attached Processor System (AP3 and Later), Operation, Maintenance, and Recovery User's Guide*

- 231-390-207, *1A ESS Traffic Measurements Features Document Switch*
- 231-390-500, *Common Channel Signaling System 7, General Description, Feature Document, 1A ESS Switch*
- 231-390-502, *Integrated Services User Part, Common Channel Signaling System 7, Feature Document, 1A ESS Switch*
- 231-390-509, *Service Switching Point, Common Channel Signaling System 7, Feature Document, 1A ESS Switch*
- 231-390-510, *800 Service, Common Channel Signaling System 7, Feature Document, 1A ESS Switch*
- 231-390-515, *Local Area Signaling Services, Common Channel Signaling System 7, General Description, Feature Document, 1A ESS Switch*
- 231-390-520, *1A ESS Switch Advanced Services Platform, Network Access Point Features*
- 231-390-521, *Network Interconnect Common Channel Signaling System 7 Feature Document, 1A ESS Switch*
- 234-010-315, *Domestic Call Irregularity Handbook*
- 234-060-210, *4ESS™ Switch, Network Switching Engineering Service and Miscellaneous Circuits*
- 234-090-001, *Network Interconnect Common Channel Signaling System Seven, Feature Document, 4ESS Switch*
- 234-090-002, *Service Switch - 800 General Description, Feature Document, 4ESS Switch*
- 234-100-000, *4ESS Switch, General Description*
- 234-100-120, *Common Channel Signaling Systems, Common Network Interface*
- 234-100-121, *Common Channel Signaling Systems, Common Network Interface (CNI), Operations Manual Introduction*
- 234-151-120, *Common Network Interface, 4ESS Switch, Task-Oriented Practice*
- 234-152-147, *CCIS Circuit Order Recent Changes (Trunk Conversion)*
- 234-152-149, *Non-CCIS Circuit Order Recent Changes (Trunk Conversion)*
- 234-160-014, *4ESS Switch, 4E13 to 4E14 Generic Retrofit*
- 235-070-100, *5ESS® Switch, Traffic and Plant Measurements*
- 235-118-248, *5ESS Switch, Recent Change Reference, 5E9 Software Release*
- 235-190-101, *5ESS Switch, Business and Residence Modular Features*
- 235-190-120, *5ESS Switch, Common Channel Signaling Services Features*

- 235-190-125, *5ESS Switch, ASP Feature Document*
- 235-190-130, *5ESS Switch, LASS Feature Document*
- 235-600-700, *5ESS Switch, Input Message Manual*
- 235-600-750, *5ESS Switch, Output Message Manual*
- 256-002-100, *Switching Products, Common Channel Signaling 7, Information Guide*
- 270--110, *CCS7 Signaling Protocol Description, Common Channel Signaling Systems*
- 270-750-401, *A-I-Net® STP System Description*
- 270-750-402, *A-I-Net STP Operations Manual*
- 270-750-403, *A-I-Net STP Maintenance Manual*
- 270-750-404, *A-I-Net STP Input Message Manual*
- 270-750-405, *A-I-Net STP Output Message Manual*
- 270-750-406, *A-I-Net STP Data Base Administration Manual*
- 270-750-407, *A-I-Net STP Reference Manual*
- 256-230-100, *Common Channel Signaling System*
- 795-100-100, *CLLI Code Description*

2. Other Sources

2.01 Following is a list of other documents related to SS7 network routing and data base requirements.

- *CCS7 MTP and SCCP Network Interconnect Feature Specification*
- *DATAPHONE® II 2500 Series, Data Service Unit User's Guide*
- PR-6A1444 *STAR Implementation Guide, 1A ESS Switch*
- IM-4A000 *4ESS Switch, Input Message Manual*
- IM-4A001 *4ESS Switch/APS, Input Message Manual*
- IM-4B000 *4ESS Switch, Input Message Manual*
- IM-4B001 *4ESS Switch/APS, Input Message Manual*
- IM-6A001 *1A ESS Switch, Input Message Manual*
- IM-6A002 *1A ESS Switch/APS Input Message Manual*

- OM-4A000 *4ESS Switch, Output Message Manual*
- OM-6A001 *1A ESS Switch, Output Message Manual*
- OM-6A002 *1A ESS Switch/APS. Output Message Manual*
- *Library Program Procedure WE® STAR Manual, Remote Office Preconditioning*
- *1A ESS Switch Translations Guide (TG 1A)*
- *4ESS Switch Translations Guide (TG4)*
- IM/OM 5D000-01 *5ESS Switch Input/Output Message Manuals*
- *5ESS Switch Translations Guide (TG5)*
- *Common Channel Interoffice Signaling*, TA14, Bell Telephone Laboratories, November 6, 1980
- TR-NWT-000246, *Bell Communications Research Specifications of Signaling System Number 7*
- TR-TSY-000024, *Service Switching Points (SSPs) Generic Requirements*
- TR-TSY-000031, *CLASS Feature: Calling Number Delivery*
- TR-NWT-000032, *CLASS Feature: Bulk Calling Line Identification*
- TA-NWT-000082, *Signal Transfer Point Generic Requirements*
- TR-NWT-000215, *CLASS Feature: Automatic Callback*
- TR-TSY-000216, *CLASS Feature: Customer Originated Trace*
- TR-TSY-000217, *CLASS Feature: Selective Call Forwarding*
- TR-TSY-000218, *CLASS Feature: Selective Call Rejection*
- TR-TSY-000219, *CLASS Feature: Distinctive Ringing/Call Waiting*
- TR-NWT-000220, *CLASS Feature: Screening List Editing*
- TR-NWT-000227, *CLASS Feature: Automatic Recall*
- Bellcore TR-NWT-000246, Bell Communications Research Specification of Signaling System Number 7
- TR-NWT-000317, *Switching System Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)*
- TR-NWT-000394, *Switching System Requirements for Interexchange Carrier Interconnection Using the ISDNUP*

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W